UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE DOUTORADO EM CIÊNCIA JURÍDICA – CDCJ
ÁREA DE CONCENTRAÇÃO: CONSTITUCIONALISMO, TRANSNACIONALIDADE E PRODUÇÃO DO DIREITO
LINHA DE PESQUISA: ESTADO, TRANSNACIONALIDADE E SUSTENTABILIDADE
PROJETO DE PESQUISA: DIREITO AMBIENTAL, TRANSNACIONALIDADE E SUSTENTABILIDADE
DUPLA TITULAÇÃO COM A WIDENER UNIVERSITY – DELAWARE LAW SCHOOL

THE PROTECTION OF CHILDREN'S DATA FOR COMMERCIAL PURPOSES IN BRAZIL FROM TRANSNATIONAL STANDARDS

ANA LUIZA COLZANI

Itajaí-SC December 2022

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE DOUTORADO EM CIÊNCIA JURÍDICA – CDCJ
ÁREA DE CONCENTRAÇÃO: CONSTITUCIONALISMO, TRANSNACIONALIDADE E PRODUÇÃO DO DIREITO
LINHA DE PESQUISA: ESTADO, TRANSNACIONALIDADE E SUSTENTABILIDADE
PROJETO DE PESQUISA: DIREITO AMBIENTAL, TRANSNACIONALIDADE E SUSTENTABILIDADE
DUPLA TITULAÇÃO COM A WIDENER UNIVERSITY – DELAWARE LAW SCHOOL

THE PROTECTION OF CHILDREN'S DATA FOR COMMERCIAL PURPOSES IN BRAZIL FROM TRANSNATIONAL STANDARDS

ANA LUIZA COLZANI

Dissertation submitted to the Doctoral Course in Legal Science of the University of Vale do Itajaí - UNIVALI, and to the Doctor of Juridical Science (SJD) of the Delaware Law School - Widener University, as a partial requirement to obtain the title of Doctor of Legal Science.

UNIVALI Superviser: Professor Dr. Osvaldo Agripino de Castro Júnior
Widener University Superviser: Professor Dra. Patty Dailey Lewis

Itajaí-SC December 2022

ACKNOWLEDGMENTS

Since I was a child, I had already walked the academic path towards the doctorate. I wasn't sure about the area, and I wasn't aware of the challenges along the way, but there was no doubt about the goal. I saw on my parents' bookshelves a whole world of possibilities. I wanted to write a lot. I wanted to make up those shelves with my ideas.

Thinking now of thanking all the people who have pushed me so far seems an even bigger mission than the dissertation itself.

My family, of course, has always been the fuel of my dreams and the support that made it possible for me to dream. They believed in me when I often doubted.

My colleagues, especially the fellows of the PPCJ-UNIVALI, who have been with me for the last 6 years as a cog of a pulsating program, have made me realize that teamwork can be very building and fun at the same time.

I also had the opportunity to be headed by Professor Dr. Paulo Márcio da Cruz, who trusted my work and taught me not only with classes but with his daily posture as a leader command to the mold of Montesquieu.

During this process of academic construction, I traveled beyond the books. I took classes in Italy; I studied for my master's degree in Spain and my Doctorate in the United States. Thanks to UNIVALI's joint effort with the partner institutions of internationalization agreements.

On this path, I gained a lot: friends, admiration for great professors, knowledge, academic humility, opportunities, and my greatest gift: my daughter.

But I also lost my father, hastily, without goodbyes, without being able to deliver to him, finally, the final version of this work. We talked so much about this dissertation, we talked about life and the reasons why we chose to study. Thank you, Dad. You do live in me, in my choices, and certainly in this job.

DEDICATION

E eu que achava que a maior conquista da minha vida seria um título, não estava errada. Mas não era de Doutora, era o de mãe.

Essa tese é para você, meu amor, minha Gabi.

Que você seja livre para ser você.

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Doutorado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, 15 de outubro de 2022.

ANA LUIZA COLZANI

Assinado de forma digital por ANA LUIZA COLZANI
Dados: 2023.07.03 17:06:36 -03'00'

Ana Luiza Colzani

Doutorando(a)

P Á G I N A D E A P R O V A Ç Ã O

DOUTORADO

Conforme Ata da Banca de defesa de doutorado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu em* Ciência Jurídica PPCJ/UNIVALI, em 07/12/2022, às quinze horas, a doutoranda Ana Luiza Colzani fez a apresentação e defesa da Tese, sob o título "THE PROTECTION OF CHILDREN'S DATA FOR COMMERCIAL PURPOSES IN BRAZIL FROM TRANSNATIONAL STANDARDS".

A Banca Examinadora foi composta pelos seguintes professores: Doutor Osvaldo Agripino de Castro Junior (Univali), como presidente e orientador, Doutor Francesco Paolo Micozzi (Universidade de Perugia), como membro, Doutor Heron Santana Gordilho (Universidade Federal da Bahia/UFBA), como membro, Doutora Eileen A. Grena-Piretti (Delaware Law School), como membro, Doutor Orlando Luiz Zanon Junior (Univali), como membro, Doutora Luciene Dal Ri (Univali), como membro, Doutor Bruno Makowiecky Salles (Univali), como membro suplente e Doutor Márcio Ricardo Staffen (Univali), como membro suplente. Conforme consta em Ata, após a avaliação dos membros da Banca, a Tese foi Aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), 07 de dezembro de 2022.

PROF. DR. PAULO MÁRCIO DA CRUZ
Coordenador/PPCJ/UNIVALI

LIST OF ABBREVIATIONS AND ACRONYMS

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

COPPA – Children's Online Privacy Protection Act

EU – União Europeia

U.S – United States

ECA – Estatuto da Criança e do Adolescente

FIPP – Fair Information Practice Principles

FTC – Federal Trade Commission

GDPR – General Data Protection Rule

MCI – Marco Civil da Internet

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

PIPEDA – Personal information protection and electronic documents act

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SUMMARY

ABSTRACT

This research is part of **the area of concentration** “Constitutionalism, Transnationality and Production of Law”, linked to **the line of research** “State, Transnationality and sustainability”, in the double degree program with Widener University – Delaware Law School (USA). It was **financed**, in part, by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) – Finance Code 001. The **general objective** of this study is to delimit transnational standards of child data protection for commercial use in Brazil. The theme has special relevance because even though data protection has been discussed in depth in recent years - driven by new regulations around the world - the focus on childhood seems to have been mitigated. Little has been produced in the doctrine about this vulnerable sector of the population that is such a rich target of the trade war for information. However, one cannot draw paths to regulation based on internal sources, as when it comes to data protection, the reality is cross-border, and new global actors delimit, in practice, how the data of millions of children are processed. In order to be able to identify children's data protection standards for commercial purposes in Brazil, the **specific objectives** of this work are to**:** (i) discuss theories on the right to privacy; (ii) specify the right to data protection in its peculiarities; (iii) understand the impacts of data collection on children's privacy, as well as the regulation of advertising; (iv) analyse transnational data protection principles; (v) identify the main parameters of data protection relating to children in Brazil, based on General Data Protection Law; (vi) identify the main parameters of data protection relating to children in the United States, based on the Children's Online Privacy Protection Act*;* and (vii) recognize the need for a transnational approach in the implementation of data protection for commercial purposes relating to children in Brazil. This work is divided into seven chapters, focusing on the above objectives. The inductive **method** is used in the investigation phase; the cartesian in the data processing phase, and the inductive logical basis in the research report, expressed in the form of this dissertation.

Keywords: Privacy; Data protection; Children; Transnational standards.

RESUMO

*Essa pesquisa está inserida na **área de concentração** de "Constitucionalismo, Transnacionalidade e Produção do Direito", vinculada à **linha de pesquisa** "Estado, Transnacionalidade e Sustentabilidade", com dupla titulação pela Widener University – Delaware Law School (EUA) e foi **financiada** em parte pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) – Código de financiamento 001. A presente tese tem como **objetivo geral** delimitar standards transnacionais de proteção de dados de criança para uso comercial no Brasil. O tema tem especial relevância pois, ainda que a proteção de dados esteja sendo exaustivamente discutida nos últimos anos - impulsionada por novas normativas ao redor do mundo - o enfoque para a infância parece ter sido mitigado. Pouco se produziu na doutrina, até então, sobre essa parcela vulnerável da população e alvo tão rico da guerra comercial por informações. No entanto, não é possível apenas traçar caminhos para uma regulamentação baseada em fontes internas, à medida que a realidade da proteção de dados é transfronteiriça e novos atores globais delimitam, na prática, como os dados de milhões de crianças são tratados. Para que possa se concluir pelos standards de proteção de dados das crianças para fins comerciais no Brasil, tem-se os seguintes **objetivos específicos**: (i) discorrer sobre teorias do direito à privacidade; (ii) especificar o direito à proteção de dados em suas peculiaridades; (iii) compreender os impactos da coleta de dados à privacidade infantil, bem como a regulamentação à publicidade; (iv) analisar os princípios transnacionais de proteção de dados; (v) identificar os principais parâmetros de proteção de dados de crianças no Brasil, a partir da Lei Geral de Proteção de Dados; (vi) identificar os principais parâmetros de proteção de dados de crianças nos Estados Unidos, a partir da Children's Online Privacy Protection Act; (vii) reconhecer a necessidade da abordagem transnacional na implementação da proteção de dados para fins comerciais de crianças no Brasil. Assim, o trabalho foi dividido em sete capítulos a responder, cada qual, por um objetivo específico. O **método** utilizado na fase de investigação foi o indutivo; na fase de tratamento dos dados, o cartesiano, e no relatório da pesquisa, expresso na presente tese, a base lógica indutiva.*

***Palavras-chave**: Privacidade; Proteção de dados; Crianças; Standards transnacionais.*

RESUMEN

Esta investigación se inserta en el ***área de concentración*** de "*Constitucionalismo*, Transnacionalidad y Producción de Derecho", vinculada a la línea de ***investigación "****Estado, Transnacionalidad y Sostenibilidad", con una doble titulación de Widener University – Delaware Law School (USA) y fue* ***financiada*** *en parte por la Coordinación para el Perfeccionamiento del Personal de Educación Superior - Brasil (CAPES) - Código de Financiamiento 001. Esta tesis tiene como* ***objetivo general*** *delimitar los estándares transnacionales de protección de datos de niños para uso comercial en Brasil. El tema tiene especial relevancia porque, aunque la protección de datos se ha discutido exhaustivamente en los últimos años, impulsada por las nuevas regulaciones en todo el mundo, el enfoque en los niños parece haberse mitigado. Poco se ha producido en la doctrina, hasta ahora, sobre esta porción vulnerable de la población y tan rico objetivo de la guerra comercial por información. Sin embargo, no solo es posible trazar caminos para la regulación basada en fuentes internas, ya que la realidad de la protección de datos es transfronteriza y nuevos actores globales delimitan, en la práctica, cómo se tratan los datos de millones de niños. Para poder concluir los estándares de protección de datos de niños con fines comerciales en Brasil, se persiguen* los siguientes ***objetivos específicos****: (i) discutir teorías sobre el derecho a la privacidad; (ii) especificar el derecho a la protección de datos en sus peculiaridades; (iii)* comprender los impactos de la *recopilación de datos en la privacidad de los niños, así como la regulación de la publicidad; (iv) analizar los principios transnacionales de protección de datos; (v) identificar los principales parámetros de protección de datos de los niños en Brasil, sobre la base de la Ley General de Protección de Datos; (vi)* identificar los principales parámetros de protección de los datos de los *niños en los Estados Unidos, sobre la base de la Ley de Protección de la Privacidad en Línea de los Niños; vii) reconocer la necesidad de un enfoque transnacional en la aplicación de la protección de datos con fines comerciales de los niños en el Brasil. Por lo tanto*, *el trabajo se dividió en siete capítulos para responder, cada uno de los cuales para un objetivo específico. El* ***método*** utilizado en la fase de investigación *fue el inductivo; en la fase de procesamiento de datos, el cartesiano, y en el informe de investigación, expresado en esta tesis, la base lógica inductiva.*

Palabras clave*: Privacidad; Protección de datos; Niños; Normas transnacionales.*

INTRODUCTION

This research is carried out in the concentration area “Constitucionalismo, Transnacionalidade e Produção do Direito”, linked to the search line of “Estado, Transnacionalidade e Sustentabilidade”, and it was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, through the Programa de Excelência Acadêmica (PROEX) as a fellow, in the Ph.D. modality.

The institutional objective of this study is to obtain the title of Doctor in Legal Science by the Doctorate Course in Legal Science of UNIVALI and the title of Doctor of Juridical Science (SJD) in Corporate and Business Law, from Widener University – Delaware Law School.

The issue of data protection has been thoroughly discussed in recent years by the impulse of new regulations, to draw clear guidelines on the right to privacy and information security. However, the focus on childhood seems to have been mitigated. Little has been produced in the doctrine, until then, about this vulnerable portion of the population and such a rich target of the trade war for information.

Algorithms work increasingly accurately and unfasten parts until then restricted to the deepest human intimacy. Still, one would be talking about a relatively recent reality. As much as information has been collected forever, it is the ability to store it, and more, to treat it, which makes recent years especially sensitive to the topic.

Today's adults probably have not had their lives tracked as they will have tomorrow's adults, from an early age. Babies are already registered in the Register of Individuals and have their biometrics collected and digital health card. Classes take place in a recorded virtual environment, with all evaluations recorded by the platforms. Cell phones are precise geolocation traces that accompany them everywhere.

This information outlines an accurate profile of the user. What are the tastes, the preferences, which diseases would be most susceptible, and what is life

expectancy? The value of this information is precious to marketing strategies. At the right time, the right announcement, just a click away from immediate desire, is every supplier's dream of products or services.

If, for an adult, the appeal of targeted advertising is highly effective, even if there is a certain awareness of the manipulative power, how crucial the direction of information can be for the formation of being, in the construction of personality, or the intellectual freedom of a child?

The use of children's data in disregard of their right to privacy may pose risks to their safety or be decisive for their opportunities (or lack thereof) in their future life. There are numerous possibilities for the use of this information that could somehow lead to discrimination, mass surveillance, media manipulation, etc.

Being the extremely current theme, not only the answers, but also the questions still lack formulation. The timing could not be more opportune. Brazil has just enacted its data protection legislation (LGPD - Law No. 13,709/2018) and there is certainly a large interpretative gap regarding the only one article dedicated to childhood.

The Brazilian data protection law is recent and its dialogue with other sources of domestic law, such as the Statute of children and adolescents, the Consumer Protection Code, and even the Federal Constitution, remains immature.

However, it is not only possible to chart paths to dialogue with other internal norms, as the reality of data protection is cross-border, and new global actors delimit, in practice, how the data of millions of children are treated.

The most visited websites and most used apps keep their databases out of the country, with their privacy policies. National law seems to survive this reality.

By understanding the need for a transnational approach to data protection and children's privacy, as well as existing gaps that could mitigate the effectiveness of protection, it will be possible to achieve the **general scientific objective of this study: sustain a children's data protection standard for commercial use in Brazil.**

The research hypotheses are:

a) The North American data protection model could be implemented in Brazil to broaden the interpretation of Article 14 of the General Data Protection Law;

b) Internal law rules, such as the Consumer Protection Code and the Statute of children and adolescents, would be enough for an extensive, sufficiently protective interpretation of children's rights to their data protection.

To validate the hypotheses or not, the research was divided into seven chapters, each containing a specific objective.

Chapter 1 aims to analyze the theoretical construction of the right to privacy and will begin with a historical view of when and how the right to privacy emerged as a social, cultural, and legal idea, contextualizing it as a modern human right.

Thus, it investigates the doctrine of different attempts to conceptualize privacy, either as a single concept or as a multiple concept. This attempt, or failure, to find a concept of privacy presupposes the scope of the application of the theme, in addition to demonstrating that the right to data privacy is only one branch of the right to privacy.

Chapter 2 specifies the right to data protection in its peculiarities, differentiating it from the right to privacy, as well as pointing out the imminent risks to the subject and the arguments contrary to its regulation

Chapter 3 aims to understand the impacts of data collection on child privacy, using a social and legal approach, addressing childhood and the special protection required of this category in the face of data privacy and the possible interference in the formation of the "self", in the construction of autonomy, self-determination and the risks to their security.

The chapter also deals with the current regulation of advertising in Brazil and defines the types of advertising that violate children's rights.

Chapter 4 is dedicated to the transnational principles of data protection, collected from Schwartz and Solove's analysis of different regulatory bases around the world, to suggest a standard of protection to be taken into account for building standards or regulations in the United States.

The work advances to Chapter 5 which addresses the main elements of child data protection and privacy in Brazil, from a dialogued reading of the General

Data Protection Law with other legal sources, such as the Federal Constitution, Consumer Protection Code, and the Statute of Children and Adolescents.

Chapter 6 seeks the same elements in the United States, from the Children's Privacy Protection Act (COPPA) from dialogue with other internal sources. As well as understand how the advertising targeting child is regulated. The approach also seeks to identify convergences and divergences with Brazilian legislation.

The North American country was chosen to integrate the analysis, together with Brazil, because the author conducted the dissertation research in immersion, in the double degree regime, with Widener University – Delaware Law School, North American University, and also attended the disciplines of Technology & the law, Advanced corporations, Legal English and Digital Law: cybersecurity and privacy in the same university.

Moreover, and more importantly, the United States emerges with important transnational actors on the subject. Among them, it is important to highlight: a) the consolidated and changing doctrine of privacy protection and data protection; b) the home of the main digital conglomerates, and c) the regulatory model with a strong impact on their agreements.

Despite this, and perhaps for this, federal regulations of data protection are much less restrictive than that of the European Union, for example, or the Brazilian Data Protection Law (LGPD). Concerning the protection of children's data, on the contrary, there is a specific law (COPPA – Children's Online Privacy Protection Act) only in the U.S.A.

In this sense, the results of the analysis of contrasts will enrich the debate on the protection given to the child about the protection of his privacy and protection of his/her data.

Finally, Chapter 7 seeks to understand the need for a transnational approach to data protection and children's privacy, as well as existing gaps that could mitigate the effectiveness of protection; to support the protection of children's data for commercial use in Brazil, appropriate to transnational criteria.

This Research Report ends with the Conclusions, in which highlighted aspects of creativity and originality in the report are presented, and the well-founded

contributions it brings to the scientific and legal community on the subject, followed by stimulation of the continuity of studies and reflections on the protection of children's data in Brazil from a transnational standard.

The method to be used in the investigation phase is inductive; in the data processing phase, the Cartesian, is the fractionation of the elements for the best individual understanding, and, for this research report the logical-inductive method is used[1].

In this thesis the Main Categories are spelled with the initial letter in capital letters and their operational concepts are presented in the text or footer when first mentioned.

[1] PASOLD, Cesar Luiz. **Metodologia da pesquisa científica:** teoria e prática. 14.ed.rev.current. and amp. Florianópolis: EMais, 2018. p.89-115.

CHAPTER 1

GENERAL THEORY OF PRIVACY

The philosophical foundations of the dichotomy between public and private go as far as philosophy itself[2], having Aristotle characterized man as a social-political animal by nature[3]. Not only because of the need for life in society as a condition of subsistence, which equates it to any other animal with limitations imposed by biological life, but mainly by the possibility of exercising political man.

The political being thus divides the sphere of the private and the public and reaches a unique facet of the human being. It is the capacity for political organization and the emergence of the city-state that creates this dimension beyond private life and own interests (*idion*), for the interests of what is common (*koinon*)[4].

And yet, as "the animal that has the gift of speech"[5], exercise, no longer through force, but through discourse, relations with the other. It is, therefore, the ability to speak, and more, to reason and persuade through this discourse that differentiates man from other animals.

It is the exposition of the, until then, intimate thoughts, or even the passage of the private to the public of these that would make possible the exchange with the like, knowing their virtues and sharing the sense of good and evil, the just and the unjust[6].

There is, however, no way to assume a single historical moment or a

---

[2] Defined from Habermas as the origin of the categories "public" and "private". HABERMAS, Jürgen. **Mudança estrutural da esfera pública**: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014, p. 97-98.

[3] ARISTÓTELES. **Política**. Tradução de Mário da Gama Kury, 3. Ed. Brasília: editora Universidade de Brasilia, 1997, p. 15. With the addition of the word "political" to the original translation as a result of the interpretation given by ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. Ed. Rio de Janeiro: Forense Universitária, 2007, p. 31-37.

[4] ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. Ed. Rio de Janeiro: Forense Universitária, 2007, p. 33.

[5] ARISTÓTELES. **Política**. Tradução de Mário da Gama Kury, 3. Ed. Brasília: editora Universidade de Brasilia, 1997, p. 15.

[6] ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. Ed. Rio de Janeiro: Forense Universitária, 2007, p. 36.

single motivation that has led to what is now understood as the right to privacy. Choosing a theoretical construction line, however, is not denying the existence of others, but only making possible a viable research delimitation.

Nor is there a universal perception of privacy, and therefore analysis demands a social delimitation. For Chapter 1 of this work, when dealing with the general theory of privacy, a look was chosen from north-American society, for two reasons: the first, because it is this thesis built on a double degree from a north-American university, having the author gone through a period of research in immersion in the country and, second, because it is the country an academic and legal reference in the construction of the right to privacy, and the first to constitutionalize it.

But then, by protecting "privacy," what is being protected? Philosophers, jurists, sociologists, and academics tried to answer this question with different theoretical approaches. There is, however, no consensus in the academic literature regarding the definition of privacy as a social object, nor of the right to privacy, as a legal application, as will be seen below.

1.1 Building privacy as a right

As complex as defining what privacy is delimiting its exact legal origin. The right to privacy in modern democratic states emerges in different parts of the world at different times and dimensions. As every right is also a product of social construction and is strictly related to politics and culture.

Therefore, it will not be reconfirmed since when the human being recognizes or exercises privacy because it is not the objective of the present work. The redemption will be from when privacy becomes legally protected when recognition of its absence.

The theoretical frameworks will be presented in chronological order to better understand the construction of the argumentation around the right to privacy, its scope, and its application.

It was from this point that the dichotomy between public and private

gained special strength as a derivation of the natural right of freedom[7]. John Locke[8] gave the property the central role of liberalism in devoting to the human being the possibility of opposing the state's intrusion, as the right that each man has to exclude others from possession and control over the proceeds of his work.

Thus, as political content, privacy appears in the liberal state through property as a space of human isolation. In this sense, John Stuart Mill[9] defined property as a limiting principle of state power control in the "sacred" life of individuals. Thus, private property is justified by the prerogative of family privacy and correlates to freedom as a possibility to the human being the exercise of the intimate sphere, which should not be coerced by the State for acts not justified by damage to the other.

> This, then, is the appropriate region of human liberty. It comprises, first, the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological[10].

Individual freedoms began to be valued and preserved as something intimate and untouchable by the State, until they ran into offense to the other person.

The constitutional recognition of the right to privacy appeared, at first, in this sense of protection of property, through the inviolability of the house and correspondence[11], as of the Constitution of the United States of 1787 (4th amendment, 1791). Reflected later in several Constitutions, such as the Brazilian Constitution, since the Constitution of the Empire of 1824, [12]as well as the

---

[7] when articulated by Aristotle, Cicero and Thomas of Aquino.

[8]LOCKE, John. **According to the civil government treaty.** Translation: Magda Lopes and Marisa Lobo da Costa. Voices Publishing House. Available at: <http://www.xr.pro.br/if/locke-segundo_tratado_sobre_o_governo.pdf> Accessed 11 Ago., 2018.

[9] MILL. John Stuard. **On Liberty**, 1859. Chapter I. Available at: <https://www.utilitarianism.com/ol/one.html> Accessed 11 Ago., 2018.

[10] MILL. John Stuard. **On Liberty**, 1859. Chapter I. Available at: <https://www.utilitarianism.com/ol/one.html> Accessed 11 Ago., 2018.

[11] RUIZ MIGUEL, Carlos, **La configuracion constitucional del derecho a la Intimidad**. Doctoral thesis. Universidad Complutense de Madrid, June 15, 1992. Available at: <https://perma.cc/5YR4-2679> Accessed 11 Ago., 2018.

[12] Art. 179. The inviolability of Civil Rights, and Politicians of Brazilian Citizens, which is based on freedom, individual security, and property, is guaranteed by the Constitution of the Imperio, by the following way. (...) VII. Every Citizen has in his house an inviolable asylum. At night one cannot enter

Constitutions of the United States of Mexico, 1917 (art. 16), Imperial Constitution of Japan of 1946 (art. 35), Constitution of the Italian Republic of 1947 (arts. 14 and 15), among many others.

The right to privacy, in this sense, opposes state power and surveillance decisions by the counterpoint of public security. Thus, it becomes a political decision to face the limits between the individual interest of keeping correspondence confidential and the domicile in the interest of the public administration, so do in cases of public interest, in the prerogative of maintaining security.

Just as liberal ideas were quite elitist - worrying about private property, which effectively belonged to a few - the first concerns about technology that reached the courts were driven by the press, when the first newspapers became periodicals and brought the reach of information – from a few – to the many.

In 1741, in England, an editor published without authorization love correspondences between the poet Alexander Pope and Jonathan Swift[13]. In 1848, in France, there was the case of the graphic reproduction of the objects of Prince Albert and Queen Victoria[14]. In both, the right to property – of letters and objects – was the argument used to ensure the right to privacy in the specific situation.

The advent of photography also introduced debates about the image of the individual. The first known case to deal with the issue was by the French Court (Civil Court of the Seine) in 1858. At the time, photographs of the actress Elisa Racher Félix, at her wake, were taken as a family memory, however, disseminated by the photographer without consent. The ruling decided to be prohibited from reproducing and advertising photographs without the consent of the person or his family[15]. Soon after, there was the creation of the French Press Law (1868), in which

---

nella, if not by his consent, or to defend him from fire, or flood; and by day will only be franchised its entry in the cases, and by the manner, that the Law determines. (...) The Secret of Letters is unusable. The Post Office is strictly responsible for any violation of this Article. BRASIL. **Constituição política do Império do Brasil**, of March 25, 1824. Available at: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm> Accessed 11 Ago., 2018.

[13] Pope v. Curl, 26 eng. rep. 608 (1741).

[14] Prince Albert v Stange 64 ER 293 (1848).

[15] RICHARDSON, Megan. **The right to privacy**. Origins an influence of a nineteenth-century idea. Cambridge University Press: 2017, p. 64-65.

it was established that "the publication, in a periodical writing, of fact relating to private life constitutes a misdemeanor punishable by the penalty of five hundred francs"[16].

A few years after the Supreme Court of Michigan (United States) granted the right to exclude a single man from the room during labor because "the painting had a legal right to privacy of her apartment at such a time and the law secures to her this right by requiring others to observe it"[17].

It was also the annoyance of the violation of family privacy by the print media that Warren, along with the then-future U.S. Supreme Court justice Brandeis, defined privacy as "the right to be left alone"[18]. The authors deduced, from the analysis of decisions of English and American courts, that privacy was already implicit as a general principle *in common law by* guaranteeing the individual his broad freedom in the exercise of the right to life[19].

The article expressed concerns about the advent of photography as new technology, and the expansion of other people's dissemination and interest through mass media. A theme is still current, as it corroborates the mass interest in new technologies and the challenges faced for the protection of the individual in this context.

Thomas Cooley also tried to define the right to privacy as "a right of complete immunity: to be let alone"[20]. Warren and Brandeis, however, had the greatest impact on the definition, inspired by the reading of the work of the philosopher Ralph Waldo Emerson, who proposed solitude as a criterion and source

---

[16] BERTRAND, André. **Droit à la vie privée et droit à l'image**. Paris: Litec, 1999. p. 3.
[17] DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881)
[18] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review** 4, no. 5: 1890, p.193– 220.
[19] Yovatt v. Wingard, 1 Jac. & W. 394 (1820); Abernethy v. Hutchinson, 3 Law J. Ch. 209 (1825); Prince Albert v. Strange, 2 DeGex & S. 652 (1849); Tuck v. Priester, 19 QB 639 (1887); Pollard v. Phot. Co., 40 Ch. 345 (1888), WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review** 4, no. 5: 1890, p.193– 220.
[20] As Cooley described the right, it was a right to be free from assault or threats of violence. As he characterized it, "The right to one's person may be said to be a right of complete immunity: to be let alone". COOLEY, Thomas. **A treatise of the law of torts**: or the Wrongs which Arise Independent of Contract. Callaghan: Michigan University, 1879. 775 p.

of freedom[21].

Certainly, they did not invent the term "privacy", but popularized its application beyond property (correspondence or domicile, for example), by approaching the guardianship of personality; especially after Brandeis' ascension to the Supreme Court, through his decisions and arguments that brought his theory closer to the jurisprudential construction of the right to privacy.

The authors counter that, even if there is the right to inviolability of correspondence, what is being protected is not only the letter itself, as the property of someone, of the unauthorized copy, for example, but it also protects, and perhaps mainly, the subjective content of feelings and emotions expressed by this – as a right to privacy[22].

As early as 1905, the Supreme Court of Georgia became the first state court to recognize the right to privacy as a freestanding right[23], and no longer only implicitly considered, citing in the decision the article of Warren and Brandeis in the reasoning.

The text is still a reference in decisions involving the subject of privacy, as it was in 1928, through the case of Olmstead v. United States,[24] in which the legality of the interpretation of conversations as incriminating evidence was discussed. The accused had the basement of his office intercepted by wiretaps that led to his conviction, without any prior judicial authorization to search. The constitutional discussion of the case was due to the alleged violation of the 4th and 5th

---

[21] According to Mason, during Brandeis' years as a student at the Harvard Law School, Emerson was Brandeis' favorite author. MASON, Alpheus Thomas. **Brandeis**: A free man's life. William s Hein & Co: Reprint edition (June 30, 2007).

[22] "It is difficult to regard the right as one of property, in the common acceptation of that term. A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully; and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry; the restraint extends also to a publication of the contents. What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself". WARREN, Samuel D; BRANDEIS, Louis D. 1890. The Right to Privacy. **Harvard Law Review** 4, no. 5: 193– 220.

[23] Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905). Available at: <http://faculty.uml.edu/sgallagher/pavesich_v.htm> Accessed 12 Ago., 2018.

[24] Olmstead v. United States, 277 U.S. 438, 473-76 (1928). Available at: <https://supreme.justia.com/cases/federal/us/277/438/> Accessed 11 Aug., 2018.

Amendments of the U.S. Constitution, which they have in its text, in its entirety:

> Amendment IV
>
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.
>
> Amendment V
>
> No person shall be held to answer for a capital or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

The final decision of the Supreme Court was from 5 votes to 4, having as a majority the position that there was no violation of the 4th amendment because the right guaranteed by it constitutes only the protection of physical search in the private space. Thus, a letter or a house is physically violated, but a conversation – the object in question – being very immaterial, would not be contemplated by the norm.

Therefore, the trial also considered that there was no violation of the 5th Amendment since the accused was not obliged to produce evidence against himself and held the conversations deliberately.

Brandeis, now a Judge on the U.S. Supreme Court, was one of the votes won. It cited in its report that the right to privacy is “the most comprehensive of rights and the right most valued by civilized men”[25].

Finally, in 1948 the right to privacy beyond property emerged through the Universal Declaration of Human Rights. Article 12 contemplates that

> No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[26].

---

[25] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[26] Adopted and proclaimed by Resolution n. 217 A (III) da Assembleia Geral das Nações Unidas em in

However, only in the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950[27] was the right to privacy beyond the inviolability of the house and correspondence, by covering, in article 8, the "right to respect for private and family life", without relating it to honor or reputation.

Thus, the issue of the private would no longer be associated exactly with something to hide by "dishonor", but for whatever reason, something that one wants to leave out of the reach of others[28].

From the scenario of change and expansion of the idea of privacy protection Brandeis' thesis gains strength, until reaching the U.S. Supreme Court again, to finally change the interpretation given by the court, through *the case* Katz v. United States[29], in which the interception of a public telephone call without a warrant was discussed.

The State, in this case, defended the legality of the act since there was no intrusion into the house, and that the public telephone was not a constitutionally protected space. Therefore, there would be no right to privacy on the pay phone, using the previous precedent.

Harvey A. Schneider, the attorney for the case, raised the argument that the debate is not about whether the public telephone is constitutionally protected by the 4th Amendment, but rather in the expectation of being that private moment, regardless of where the fact happens. Even if the phone is public, with the

---

Dec. 10, 1948. Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos**, em 10/12/1948. Available at: <http://www.ohchr.org/EN/UDHR/Pages/ UDHRIndex.aspx>. Accessed 25 Mar., 2018.

[27]UNITED NATIONS. **Convention for the Protection of Human Rights and Fundamental Freedoms** on 04/11/1950. Available at: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Accessed 25, Mar., 2018.

[28] Any country that participates as part of global community and is a signatory of various treaties is expected to protect individual privacy". International privacy policies: 1. Organization for economic cooperation and development (OECD) Guidelines on the protection of privacy and transborder flows of personal data (1980); 2. U.N. Guidelines for the Regulation of computerized personal data files, G.A. Res. 45/95; 3. Convention for the Protection of Individual with regard to automatic processing of personal data, jan. 1, 1981. Europ. T.S. n. 108,; 4. Directive 95/46/ED of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.K (l 281); 5. Asia-Pacific economic cooperation (APEC) privacy framework (2005).

[29] Katz v. United States, 389 U.S. 347 (1967). Available at: <https://supreme.justia.com/cases/federal/us/389/347/> Accessed 11 Aug., 2018.

interlocutor having the perception that no one else is listening to it, that moment should be considered private. Oppositely, even if you are at home, in a connection, when you open the windows and speak loudly, the interlocutor knows – or may have the expectation – that someone else will hear you. Thus, the conversation would not be in the same way protected as that of the previous example, by the renunciation of the right by the guardian in that context.

It would not mean, however, that the guardian was resigning from all his privacy. The limits of what is either to be private or not are identified only in the specific case and do not exceed it.

Nor would it mean that any conversation could ever be intercepted, only that, to do so, the legal requirements required by the amendment should be present for the proper warrant.

Katz's lawyers argued, then, that the text of the 4th constitutional Amendment should be read in literalness[30] especially when it quotes "to the inviolability of their people". Meaning, then, that protects from the external search, without justification or legal authorization, not only the property, but also the person in its intimacy, subjectively and immaterially. So, privacy would haunt the person, not the thing:

> And that whether or not, he's in a space when closed by four walls, and a ceiling, and a roof, or an auto-mobile, or any other physical location, is not determined of the issue of whether or not the communication can ultimately be declared confidential.
>
> We think that the right to privacy follows the individual[31].

In addition to being a breakthrough for the theory of privacy protection and its expansion beyond property, it is also the first time that expectation has been

---

[30] And we would base our contention upon this by reading or literal reading of the Fourth Amendment. I respectfully call the Court's attention that the Fourth Amendment after paraphrasing a little bit here, but it says people have a right to be "Secure in their persons." That is the very first item of protection that is contained in the First Amendment. It says persons of the Fourth Amendment. It says persons then it says houses. SCHNEIDER, Harvey A... **Official transcript of the trial section**, 00:25:08, Available at: <https://apps.oyez.org/player/#/warren15/oral_argument_audio/15388> Accessed 11 Ago., 2018.

[31] SCHNEIDER, Harvey A... **Official transcript of the trial section**, 00:13:32, Available at: <https://apps.oyez.org/player/#/warren15/oral_argument_audio/15388> Accessed 11 Ago., 2018.

consolidated as a parameter to recognize the invasion of privacy, until today adopted by the U.S. courts, present in the vote of Judge John Marshall, for the case in question.[32]

In later writing on the backroom of the case, Harvey A. Schneider[33] delegated to technological advances the change of position of the court. He brings as an example a situation in which the public agent, although without a mandate, ends up listening to a conversation in the street and that, for the previous position, was circumstantial and would not transpose the sphere of the private. The person, in public, could get some idea of the possible exposure he was undergoing. On the contrary, however, the use of the recorder for wiretaps, in which, in this case, the technology does not allow to have expectation of exposure, and therefore would not be legitimate without prior judicial authorization.

Brandeis was able to expand his role in building the application of the right to privacy by judging favorable to the constitutional affront in the case, winning his position by 7-1. It was considered that privacy exceeds the physical space of the house or correspondence and affects the protection of the person in his intimacy. Therefore, no matter where you are, at home or in a public space, the individual will carry with him an inviolable intimate sphere.

This decision became the basis for reasoning for subsequent cases[34] that consolidated the right to privacy as a constitutional right, especially enshrined in the 4th amendment of the U.S. Constitution.

A year later, Congress enacted a law regulating electronic surveillance, through which controls were established more restricted to the government's

---

[32] The "reasonable-expectation-of-privacy" test currently employed by the Court to determine the applicability of the Fourth Amendment to a particular situation was first articulated in Justice John Marshall Harlan's concurring opinion in Katz v. United States, 389 U.S. 347 (1967).

[33] SCHNEIDER, Harvey A. Katz v. United States: **The Untold Story**. 2009. Available at: <http://www.mcgeorge.edu/Documents/Publications/06_Schneider_Master1MLR40.pdf> Accessed 12 Ago. 2018.

[34] PROSSER, William L. Privacy. **California Law Review**, vol. 48. August 1960, n. 3, p. 383. Available at: <https://doi.org/10.15779/Z383J3C> Acessed 15 Ago., 2019. Also in Katz v. United States, 389 U.S. 347 (1967) Harlan, J., concurring.

clamping and recording methods[35].

Several constitutions have since expressly incorporated this immaterial meaning given to privacy, such as that of Brazil, promulgated on October 5, 1988[36], of South Africa and South Korea. In other cases, although there is no mention, there is implicit recognition given by the courts, such as in Canada, France, Germany, Japan, and India[37].

In addition, of course, there are countless laws, guidelines, recommendations, etc., that protect some aspects of privacy around the world. In this regard, it is worth mentioning the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, da Organization for Economic Cooperation and Development" (OECD) of 1980, which undertook the debates of the most recent – and probably the most influential – legislation on contemporary data privacy, for the entire European Union (EUGDPR).

The concern with privacy and its evolution does not overlap with the passage of time to the definition previously given. On the contrary, the scope of the application is expanded. If, at first, as seen, the violability of the letters was a major concern, today it is generally expanded to correspondence: exchanges of messages by electronic means, such as emails or conversation applications.

As well as advancing beyond property, by becoming an autonomous right that also protects the autonomy of the individual.

The issue remains on the agenda as an open debate to define how far the

---

[35] Title III of the Omnibus Crime Control and Safe Streets Act of, pub. L. 90-351, § 802 (1968).
[36] *the privacy, private life, honor and image of people are inviolable*
[37] Although Canada's Charter of Rights and Freedoms does not explicitly protect a right to privacy, the Supreme Court of Canada has interpreted it to imply such a right. Privacy and Human Rights, 323. The Constitutional Court in France declared in 1995 that the French constitution has an implied right of privacy. Privacy and Human Rights, 463-64. Germany's Basic Law protects the privacy of communications, and the Federal Constitutional Court in 1983 recognized the protection of a person's "right to informational self-determination" under Basic Law (Grundgesetz), art. 10 (1949). See Federal Constitutional Court, decision of Dec. 15, 1983, 1 BvR 209, quoted in Privacy and Human Rights, 480. Although the word "privacy" does not appear in Japan's constitution, the Supreme Court has recognized a right to privacy since 1963. Privacy and Human Rights, 620. Likewise, even though privacy is not mentioned in India's constitution, the Supreme Court of India has declared, "The right to privacy has since been widely accepted as implied in our Constitution." Distt. Registrar & Collector, Hyderabad & Anr v. Canara Bank Etc, [2004] INSC 668, apud SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 3.

4th Amendment in the U.S. amendment reaches in the protection of man's privacy.

Since 1970, two decisions based on Katz's case law have established that the “reasonable expectation of privacy” does not apply to information shared with third parties[38]. The first had as an object the telephone tapping by the telephone company, and the second, the tracking of the user's bank details by the bank itself. In both cases, it was understood that companies could share this information with third parties, because the consumer was aware and voluntarily accepted the risk of this when hiring. The theory of risk, brought from civil law, would apply to cases.

Thus, the precedent was opened that, in the United States, a government entity could obtain such records claiming to be necessary for the investigation, and the company, by providing it, would not be violating consumer privacy.

In 1986 a statute called the Electronic Communications Privacy Act (ECPA) entered into force[39], with the expansion of the protection of correspondence to also cover electronic means such as e-mail. However, the lack of updating of the legislation is a critical point to its effectiveness these days[40].

Recently, in Carpenter v. United States[41], it was discussed whether the search and seizure, without legal authorization, of phone records and the geolocation of mobile phones for the purposes of criminal investigation would be an affront to the right of privacy, then overturning the previous precedent.

The investigation in question was tracked for 127 consecutive days, having all the steps monitored. The state defender claimed that – following the argument of the risk from the previous precedent – when a citizen buys a cell phone is aware that it may eventually be being tracked by it, and that this information is collected all the time by the telephone company to provide the contracted service. That is, knowing the person that the cell phone depends on geolocation to work, they would be aware that this data is collected.

---

[38] See Smith v. Maryland, 442 U. S. 735, 743–744 (1979); United States v. Miller, 425 U. S. 435, 443 (1976).
[39] 18 U.S.C. § 2518 (Electronic Communications Privacy Act of 1986).
[40] SOLOVE, Daniel. **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011, p. 11.
[41] Carpenter v. United States, 585 U.S. (2018).

As a counter-argument, it was understood that the risk theory could not be applied in the delivery of personal information transferred to third parties, even if there is a contract with this specificity, for two different reasons: the first is that "consent" is sometimes neither voluntary nor even clear, since it is a contract of access with little or no flexibility of modifications by the consumer; secondly, the data is given to a specific company for specific purposes, without, however, giving up full control of this information, such as for the sale of third parties, for example.

The expansion of technology, from previous jurisprudence to the present day, was also pointed out as an argument for breaking the precedent:

> Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? Smith and Miller say yes it can—at least without running afoul of Katz. But that result strikes most lawyers and judges today—me included—as pretty unlikely[42].

The court then, by 5 votes to 4, returning to the argument of Katz's jurisprudence, pondered that when buying a cell phone, the expectation is that the company has its geolocation, but not that it uses it as a form of screening or surveillance. If you can't break into a person's home or put a bug in a room without court authorization, you can't trace them in their room, for example, through their cell phone.

However, it is not yet entirely clear what "expectation of privacy" means as a parameter of application or not of the 4th amendment. Judge Gorsuch, defeated vote, questioned, “why is someone’s location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know, and the Court does not say”.

While Judge Thomas, also defeated vote, used the argument that the case should be guided by the ownership of what was researched. By that logic, the information would not belong to Carpenter, but to the telephone company[43].

It remained clear then that the argument that the right to privacy is based

---

[42] Carpenter v. United States, 585 U.S. ___ (2018). Dissent (Gorsuch).
[43] Carpenter v. United States, 585 U.S. ___ (2018). Dissent (Thomas).

on property is still relevant, although the court, for now, remains in the parameter of expectation to limit what is protected by the right to privacy.

Thus, the idea of privacy did not exceed the meaning given in ancient Greece, as a family limitation. Nor has it ceased to be the secret kept in correspondence. Nor the intimacy of the house. But today it also has new meanings, as will be demonstrated in this work.

1.2 Theories of the conceptualization of the right to privacy

As Westin[44] observed, “few values so fundamental to society as privacy have been left so undefined in social theory”. Just like the right to "freedom" or "dignity", privacy is a fairly broad and vague term. Conceptual boundaries relate to a multitude of contexts, and “means so many different things to so many different people that it has lost any precise legal connotation that it might once have had”[45].

And that’s the major challenge in protecting privacy, “is that nobody seems to have any clear idea what it is”[46]. However, this does not render the attempt useless. On the contrary, it is not possible to be clear about the actions necessary to promote a right if we cannot at least determine the limits of its application.

Concomitantly with the construction of the right to privacy as an autonomous, constitutional, and, finally, human right; there was also an expansion of applications and meanings. The first idea of being just a right to be left alone by the State soon encountered barriers when confronting technological modernity.

The camera – which fueled Warren and Brandeis' concerns in their 1890 article – was not necessarily a violation made by the state, but with the potential to be by other individuals as well. In this case, the first paradox was born: the right to privacy becomes not only a claim of non-interference of the State in the individual's life, but also the right to seek the protection of the individual for the protection of the

---

[44] WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967, p. 7.
[45] MCCARTHY, J. Thomas. **The Rights of Publicity and Privacy.** §5.59 (2d ed. 2005).
[46] THOMSON, Judith Jarvi. **The Right to Privacy**, in Philosophical Dimensions of Privacy: An Anthology 272, 272 (Ferdinand David Schoeman ed., 1984).

right. The negative right (of non-intrusion) becomes also positive (of protection)[47][48].

The reference article sought to understand the meaning of privacy and its relevance as a right applied to common law. In 1960, Prosser drafted his article "Privacy"[49], another theoretical reference on the subject, analyzing hundreds of cases from the inspiration of Warren and Brandeis' previous work.

However, it was Westin[50] in 1967 who produced one of the most important works on the subject, at the forefront of a wave of privacy studies that grew from the late 1960s and accelerated, again, from the mid-1990s with the rise of the internet, and which remains exponential to this day[51].

The work elucidates the meaning and importance of privacy that inspired many of the later written works. Westin identified several “criteria for weighing conflicting interests”, in chapter 14 of his work, to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy, which served as the basis for the construction of the “Fair Information Practice Principles (FIPPs)”[52].

The five principles of data protection in the Code of Fair Information Practices formulated by Westin and others, in 1973, have been expanded to eight in the" Guidelines on the Protection of Privacy and Transborder Flows of Personal

---

[47] GAVISON, Ruth. Privacy and the limits of law. **The Yale Law Journal**, vol. 89, n. 3 (Jan., 1980) p. 421-471, p. 438. Available at: <http://www.jstor.org/stable/795891> Accessed 10 Aug., 2018, p. 438.

[48] Again it is necessary to emphasize that this construction does not erase the previously given meaning. The state's vigil in exchange for alleged security is still extremely important. Debates about the limits of state intrusion or the legality of certain actions that clearly happen with the use of technology for population surveillance are very current and important, even if it is not the subject of the present work.

[49] PROSSER, William L. Privacy. **California Law Review**, vol. 48. August 1960, n. 3, p. 383. Available at: <https://doi.org/10.15779/Z383J3C>. Accessed 15 Aug., 2019

[50] WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.

[51] SOLOVE, Daniel. The Legacy of Privacy and Freedom, vii, in PROSSER, William L. Privacy. **California Law Review**, vol. 48. August 1960, n. 3, p. 383. Available at: <https://doi.org/10.15779/Z383J3C>. Accessed 15 Aug., 2019. Also in Katz v. United States, 389 U.S. 347 (1967) Harlan, J., concurring.

[52] U.S. DEPARTMENT OF HOMELAND SECURITY. **PRIVACY POLICY GUIDANCE MEMORANDUM**. Washington, DC. Memorandum Number: 2008-01. Available at: <https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf> Accessed 13 Jan., 2022.

Data" by the Organization for economic co-operation and development (OCDE)[53] and now support the majority of national data protection laws around the world[5455].

Since then, there have been many theories on the subject. Most theorists, when trying to conceptualize the word "privacy", look for a group of necessary and sufficient elements that distinguish the term from another conception. That is, trying to create a category for privacy by detaching it from others, such as autonomy or freedom, and identifying the theoretical barriers between them[56].

To confirm or not the accuracy of the definition, it is sought by its coherence and logic from what common sense would classify as privacy and puts it to proof from the definition previously given. The contemporary use of expression should approach the unique concept given by theory.

As a way of organizing the main theories, Solove[57] classified them into six different approaches, which will be dealt with here individually: (1) the right to be let alone—Samuel Warren and Louis Brandeis's famous formulation of the right to privacy; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood—the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life.

Sometimes the concepts overlap, but for each one, the author evidences a distinct perspective on privacy, as well as criticisms about extremely broad or very strict concepts, as will be seen below.

---

[53] Available at: <https://www.oecd.org/sti/ieconomy/15590254.pdf> Accessed 25 Aug., 2022.
[54] ELLIOTT, Margaret S. Examining the Success of computerization movements in the ubiquitous computing era: free and opensource software movements in LLIOTT, Margaret S.; KRAEMER, Kenneth L. Computerization movements and technology diffusion: from mainframes to ubiquitous computing. **INFORMATION TODAY**, Inc: Medford: New Jersey, p. 351.
[55] The principles relating to data protection will be explained in Chapter 2 an 4.
[56] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 14.
[57] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 12-13.

1.2.1 The right to be left alone

Since Warren and Brandeis' article, the "right to be left alone" is still the most influential concept for defining privacy. For the U.S. court, as seen in the decisions of the first part of this chapter, it was from this the foundation of the right to privacy in the United States. There is no single book on the subject that does not refer to this.

The authors and their theory on privacy as a right even influenced the recognition of the constitutional right to privacy, not only in the United States, but in several other countries[58].

The concerns that inspired the article were, as seen earlier, by the media's exposure of gossip that would be private and family affairs. For authors, the right to privacy “is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all”[59].

Warren and Brandeis argued that the “common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others”. Being the “right to be let alone” is a “general right to the immunity of the person, the right to one’s personality”[60].

Thus, the article did not intend to bring a definition to privacy, but to point out that the right to privacy was already implicit in several decisions in common law, and what possible paths the theme could take. In this sense, it was extremely avant-garde and very important for the development of the theories that came later[61].

However, the concept brought in in the article is quite broad and does not specify its implications or in what circumstances people should "be left alone".

---

[58] SOLOVE, Daniel.; ROTENBERG, Marc. SCHWARTZ, Paul M. **Information Privacy** Law 31 (2d ed. 2006).
[59] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review 4**, no. 5: 1890, p.205.
[60] WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review** 4, no. 5: 1890, p. 207.
[61] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 18.

The vagueness of the expression suggests a non-intervention of the State. However, the right to privacy today seeks state intervention, in the sense of legal protection against the intrusion of other individuals, which would be a paradox of the initial idea of distancing the State from the private sphere[62].

This concept resembles a type of immunity or seclusion, which could be used broadly for any unlawful conduct directed at the individual, which would remove him from his state of "peace", thus being insufficient to characterize the application of the right to privacy.

1.2.2 Limited access to the Self

Although it approaches the idea of being left alone, limited access to the self has greater scope than the loneliness or seclusion of the primary concept. Limiting access goes beyond isolating itself from others to include an important aspect which is the established limits.

Solove highlights authors, such as Godkin[63], from the late 19th century, who had observed man's need to have the recognition of the right to keep to himself some subjects and to what extent they could be observed or opened to the public. In addition to contemporary authors who have brought their own definitions that are grouped from this category:

To Bok[64], “the condition of being protected from unwanted access by others—either physical access, personal information, or attention”. To Gross[65], “the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited”. And according to Haag[66],

> privacy is the exclusive access of a person (or other legal entity) to a realm of his own. The right to privacy entities one to exclude others from (a)

---

[62] GAVISON, Ruth. Privacy and the limits of law. **The Yale Law Journal,** vol. 89, n. 3 (Jan., 1980) p. 421-471, p. 438. Available at: <http://www.jstor.org/stable/795891> Accessed 10 Aug., 2018.
[63] GODKIN, L., E.L. Libel and Its Legal Remedy. **12 Journal of Social Science** 69, 80 (1880).
[64] BOK, Sissela. **Secrets**: On the Ethics of Concealment and Revelation 10-11 (1983).
[65] GROSS, Hyman. The Concept of Privacy. **43 New York University Law Review** 34, 35-36 (1967)
[66] HAAG, Ernest Van Den. On Privacy in **Nomos XIII**: Privacy 149, 149 (J. Roland Pennock & J. W. Chapman eds., 1971).

> watching, (b) utilizing, (c) invading (intruding upon, or in other ways affecting) his private realm

Or yet, as defined by Allen[67], "a degree of inaccessibility is an important necessary condition for the apt application of privacy".

It is possible to observe some distinctions in the idea of a limitation to the self. While some see it as an individual choice of control over who has access to themselves, others perceive it as an existential condition, such as O'Brien[68].

For this author, not all privacy would correspond to access control as an individual choice, since some types of privacy are accidental, compulsory, or even involuntary[69].

Solove's criticism of this privacy categorization is especially due to the lack of clarity about what degree of access is required to constitute a violation of privacy. This is because, between having no access to absolute access there are many possibilities of violation and the limits are unclear. Again, the concept suffers from being too broad and vague.

Criticism also goes to the opposite level, of being too narrow, as it happened in Gavison's concept[70], in which it determines limited access in "three independent and irreducible elements: secrecy, anonymity, and solitude". Thus, the concept of access restricts privacy to matters of withdrawal (solitude) and concealment (secrecy, anonymity), and excludes other forms of violation[71].

---

[67] ALLEN, Anita. **Uneasy Access**: privacy for Women in a Free Society. Rowman & Littlefield Publishers, 1988.
[68] O'BRIEN, David. **Privacy, Law, and Public Policy**, 15, 16 in SOLOVE, Daniel. Understanding privacy. Cambridge, Massachusetts: Harvard University Press. 2008, p. 19-20
[69] O'BRIEN, David. **Privacy, Law, and Public Policy**, 15, 16 in SOLOVE, Daniel. Understanding privacy. Cambridge, Massachusetts: Harvard University Press. 2008, p. 19-20
[70] GAVISON, Ruth. Privacy and the limits of law. **The Yale Law Journal,** vol. 89, n. 3 (Jan., 1980) p. 421-471, p. 438. Available at: <http://www.jstor.org/stable/795891> Accessed 10 Aug., 2018, p. 433.
[71] As will be best demonstrated in the typology presented at the end of the chapter.

1.2.3 Secrecy

Maybe the first popular idea about privacy is the secret. So much so that the fallacy of "I have nothing to hide" is a common discourse when placing privacy on the opposite side of surveillance by "state security"[72].

The secret may be something to hide, to isolate one from the other. In this sense, the secret is a form of limitation of the other over the individual, as well as the previous item.

However, through the economic analysis of law, Posner treats privacy as a tool for selecting individual information to sell the best version of himself with a certain expectation of return. That is, privacy would serve as a power to manipulate information about a person before others, the “power to conceal information about themselves that others might use to [the individuals’] disadvantage”[73].

Posner[74] also presents the property as the realization of the protection of the right to privacy, stating that personal information is consumer goods and that privacy (or the opposite, curiosity), is an intermediary asset to achieve or protect it[75].

The secrecy element incurs both the distancing of others through isolation, as in manipulation, or power, before others about what is to be kept isolated, in secret, and what is desired to be revealed. It then permeates from isolation to the active participation of the individual. This dual feature will be addressed in the

---

[72] Topic will be addressed in chapter 2.3.2.

[73] POSNER, Richard. The Economics of Justice. **Harvard University Press**. January 1, 1981, p. 271.

[74] People invariably possess information, including facts about themselves and contents of communications, that they will incur costs to conceal. Sometimes such information is of value to others: that is, others will incur costs to discover it. Thus, we have two economic goods, "privacy" and "prying." We could regard them purely as consumption goods, the way economic analysis normally regards turnips or beer; and we would then speak of a "taste" for privacy or for prying. But this would bring the economic analysis to a grinding halt because tastes are unanalyzable from an economic standpoint. An alternative is to regard privacy and prying as intermediate rather than final goods, instrumental rather than ultimate values. Under this approach, people are assumed not to desire or value privacy or prying in themselves but to use these goods as inputs into the production of income or some other broad measure of utility or welfare economic analysis to proceed. POSNER, Richard. An economic theory of privacy. **Georgia Law Review**, 3/1978, 9. 393-422, p. 394. Same meaning in POSNER, Richard. Privacy, secrecy and reputation. In: **Buffalo Law Review**, 28 (winter) 1979. 9 1-55.

[75] Corroborates with similar analysis LESSIG, Lawrence. **Code and Other laws of cyberspace**. Basic Books: New York, 1999, p. 142-163.

typology of privacy (topic 1.3).

The main criticism of the concept comes from the fact that the secret, once revealed, will never be deprived again. The right to privacy, however, is not only a preventive measure. It also has a guard about facts that have already occurred. Therefore, it is not possible to conceive that secrecy is synonymous with privacy.

Furthermore, “secrecy is certainly not coextensive with privacy; secret information is often not private (for example, secret military plans), and private matters are not always secret (for example, one’s debts)”[76].

Many subjects are not exactly secrets, but still, the individual does not wish to expose them indistinctly, for various reasons. To admit it as such would put her in opposition to advertising, a theoretical fallacy as will be dealt with a in specific topic[77].

1.2.4 Control over personal information

Thus, the control of personal information arises: even if information has been revealed, control over it remains to the individual. Disclosing a photo, for example, to a certain group of people does not make that photo public. The expectation of control (along the lines of the jurisprudence of the U.S. Supreme Court) may be that this photo does not go beyond the group's boundaries.

For Westin[78], “privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”.

Control of information would again be based on the property right. The individual would be the owner not only of his material goods, but also of his information, because it fruits his development. Therefore, it would have control over it

---

[76] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 24.
[77] Chapter 2, item 2.3.3
[78] WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.

from Locke's[79] liberal theory, that each one owns the fruits of his labor.

When thinking about intellectual property, the theory of property is easily shaped by protecting the expression of ideas, even if not realized as a material object.

However, the information is not physically safeguardable as other assets. Although intellectual property is also in a more subjective sphere, it is protected only when physical manifestation. It is necessary a record, a clear exposition of the manifestation of that idea.

The information is released for different purposes. Sometimes a telephone number is given for one purpose, which ends up being passed on to another. If the phone number was someone's property, how to value it? Can the person get the information back? Intellectual property is tangible. The information is not.

In addition, the information is the result of the work not only of those who produced it, but often also of those who received it, stored it, related it with other information, etc. Is the other the owner of this added information generated based on the information initially collected? As Solove[80] analyzed, “for instance, the value of personal information for advertisers and marketers emerges in part from their consolidation and categorization of that information”.

Again, it would be very restrictive to think about privacy on this prism. On the other hand, to think that privacy is the total control of all information exchanged with anyone is too broad, since not all information about the person is part of their intimacy or what they would like to keep under privacy.

1.2.5 Personhood

Solove[81] highlights the theories of privacy that come together as a way to

---

[79] LOCKE, John. **Second Treatise of Government** §27, at 19 (1980) (1690).
[80] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 25.
[81] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 29-34.

protect the personality upon Warren and Brandeis's notion of "inviolate personality".

It overlaps with some of the ideas already exposed, because it seeks, from the definition of the violation of personality to respond to the importance of privacy, what aspects of the self should have limited access, and what information should be controlled.

However, it finds its independence from other theories because it is constructed from a specific purpose of protecting the integrity of personality.

According to Reiman[82], the right to privacy "protects the individual's interest in becoming, being, and remaining a person". Therefore, it composes one's own personality.

On the contrary, the individual when being watched behaves based on the expectations of that observes him.

> Threatening a man with penalties or taking away his stick are both direct interferences that would prevent a man from beating his donkey. But if he stops simply because he is being watched, the interference is of a quite different kind. He could continue if he chose; being observed affects his action only by changing his own perception of it. The observer makes the action impossible only in the sense that the agent now sees it in a different light, through the eyes, as it were, of the observer[83].

Being watched brings a new awareness of the self. A consciousness from the eyes of another person, fixed as an object, "with limited probabilities rather than infinite, indeterminate possibilities"[84]. By being aware of the interest of the other, the individual restricts his choices, and thus also limits his freedom[85].

This would be a necessary condition for self-knowledge – to know oneself as an objective of scrutiny, since this observation builds, to some degree, the self.

By denying his free development while trying to hide his "real self" from the

---

[82] REIMAN, Jeffrey H.. Privacy, Intimacy, and Personhood in SCHOEMAN, Ferdinand D. **Philosophical Dimensions of Privacy:** an anthology, CAMBRIDGE*:* Cambridge University Press, 1984, p. 223-244.

[83] BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988, p. 272

[84] SARTRE, J.-P. L'etre et le neant (Paris, 1953), Part 3, Le pour-autrui. In BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988, p. 273.

[85] SARTRE, J.-P. L'etre et le neant (Paris, 1953), Part 3, Le pour-autrui. In BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988

domination of the one who observes him, Sartre characterizes the “schizoid”. “The schizoid cannot believe fully in his own existence as a person. He may need to be observed in order to be convinced that he exists, if only in someone else's world”. Thus, no matter how observation occurs, but the relationship between observing and being observed, it would necessarily bring resentment to be what the other perceives that it is, without full freedom of choice[86].

Benn[87] evaluates this idea of limiting privacy as a restriction of freedom of personality development by Sartre's observation, since

> even if it were true That my consciousness of my own infinite freedom is shaken by my being made aware that in the eyes of another I have only limited possibilities, still if I am not free, it is not his regard that confines me; his regard only draws my attention to a truth I was able formerly to disregard. And if I am free after all, then his regard makes no difference.

Not only from philosophy emerges the idea of privacy as personhood. Solove notes that the U.S. Supreme Court “has conceptualized the protection of privacy as the state’s noninterference in certain decisions that are essential to defining personhood”[88], especially in cases that involve decisions relating to marriage, procreation, contraception, family relationships, and child-rearing[89]. Thus, directly connected to the right of freedom and private autonomy.

However, again the criticism falls on the breadth of the theory, which fails to conceptualize one's own personality. What would be part of personhood, how it consolidates, or what possible influences of privacy are not topics that are easy to exploit.

In addition, not everything that is part of common ideas about personality is, in fact, private. Much of what is understood as personhood is exposed to the public. For example, “an artistic work is frequently an expression of the deepest

---

[86] From SARTRE, J.-P. L'etre et le neant (Paris, 1953), Part 3, Le pour-autrui. In BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988, p. 273-274.
[87] BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988, p. 274.
[88] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 30.
[89] As in Griswold v. Connecticut; Eisenstadt v. Baird; Roe v. Wade; Planned Parenthood v. Casey.

recess of an artist's existence, yet it is often put on public display"[90], without this being considered an injury to the right to privacy.

1.2.6 Intimacy

Theories that treat privacy as intimacy starts from the value of the development of relationships between people. Thus, it differs from personhood by expanding the idea of personal development to the relationship with others.

Intimacy would take place at different levels depending on the choice of revelation that the individual has in each of his relationships with others. "By focusing on the relationship-oriented value of privacy, the theory of privacy as intimacy attempts to define what aspects of life we should be able to restrict access to, or what information we should be able to control or keep secret"[91].

Thus, the choice of whom to share emotions, beliefs, or emotions with would define the degree of intimacy and, consequently, of established privacy.

The problem with this kind of conceptualization is to restrict privacy to just one facet of what it can be. Choosing who to share with, or what to share information with each person you relate to, doesn't cover all possibilities for privacy violations. The greatest example is probably the violation of personal data, in which the leak can be a violation of privacy without, however, being linked to any affective or friendship relationship.

On the other hand, the idea of privacy as intimacy can be very vague, because there is no clear delimitation of its scope, which seems to be merely an exchange of terms, maintaining the inaccuracy of the limits[92].

---

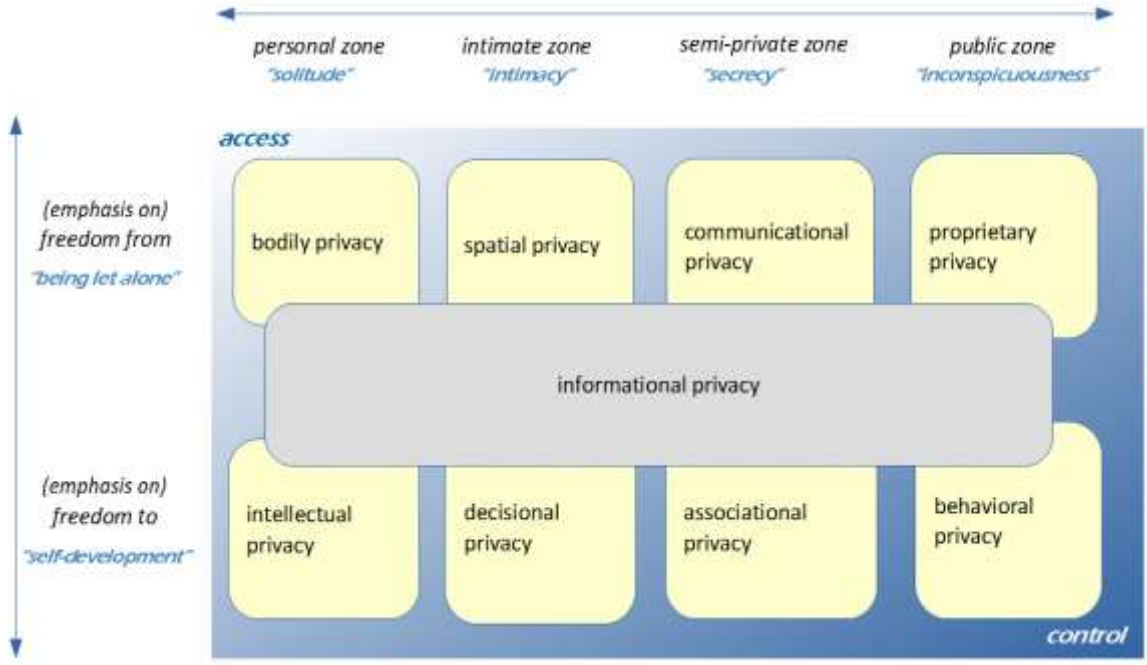
[90] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 32.
[91] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 34.
[92] SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008, p. 37.

1.3 Typology applied to privacy

Several other classifications have already been proposed on the subject, as seen. However, the following proposed typology aims to encompass all types previously foreseen from contemporary and comparative analysis, when understanding the multiple ways in which privacy can be presented, so that there are also multiple and broad ways to protect it.

Therefore, the proposal of Bert-Jaap Koops, professor of technology and regulation at Tilburg University - Tilburg Institute for Law, Technology, and Society (TILT), will be adopted as a theoretical framework for the meaning of the right to privacy, which, together with its group of Ph.D. and Postdoctoral students, elaborated a typology based on the analysis of contemporary legal protection of the right to privacy in nine countries (United States, Canada, United Kingdom, Netherlands, Germany, Czech Republic, Poland, and Slovenia)[93].

Figure 1 – Taxonomy



[93] KOOPS, Bert-Jaap; NEWEKKI, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom; GALIČ, Maša, A typology of privacy (March 24, 2016). **University of Pennsylvania Journal of International Law 38(2)**, p. 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, p. 2. Available at: <https://ssrn.com/abstract=2754043> Accessed 25 Mar., 2018.

The analysis resulted in the image above, which contains different dimensions and interpretations that will be reported below.

1.3.1 Dimensions[94]

The typology brought dimensions in eight different classifications of right to privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavior), in addition to the ninth (informational) overlapping with the others.

The horizontal dimension derives from Alan Westin's study of privacy protection by us courts, then identifying what he called "the four states of privacy"[95]: solitude, intimacy, anonymity, and reserve.

There are also different perspectives from the personal area to the public area (left to right), passing through the intimate and semi-private areas.

Thus, total isolation (personal zone) is represented by loneliness, as being the most complete state of privacy that an individual can achieve. The separation of the individual from the "others", is physical and psychological, far from what Westin [96] called "psychological intruders", such as the belief in a certain god or supernatural forces, for example, that could exercise some kind of authority.

The second state of intimacy (intimate area) corresponds to the intimate relationships of loving relationships, between family members, friends, and co-workers. It results, therefore, in close contact between these small groups with a high degree of confidence.

Westin called it "anonymity"[97], but the Authors preferred the term secrecy[98]

---

[94] The interpretation given in this item and in the next ones correspond to the analysis of the article: KOOPS, Bert-Jaap; NEWEKKI, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom; GALIČ, Maša, A typology of privacy (March 24, 2016). **University of Pennsylvania Journal of International Law 38(2)**, p. 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, p. 2. Available at: <https://ssrn.com/abstract=2754043> Accessed 25 Mar., 2018.
[95] WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.
[96]WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.
[97]WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.
[98] See picture.

to represent the semi-private area. It would be the state of privacy in which, even being in public places, the individual still finds freedom to act and communicate without being identified or monitored.

Finally, the state of privacy closest to the public area: discretion (reserve, by Westin), in the idea of going unnoticed in public environments.

In the vertical dimension, there is a spectrum between negative freedom (of being left alone) and positive freedom (for self-development) on privacy. It is important to connect this idea to those already exposed in this chapter. Certainly, privacy while the "right to be left alone" has not lost its meaning.

Privacy can still be a negative freedom. But it is also a positive freedom of self-development. And this, perhaps, is the difficulty in its understanding: to understand it also in its social aspect.

There is also a third dimension (diagonal), dependent on the other two, between access and control. The first corresponds to restricted access to some information, while the second deals with the control of this information after access has been granted. They correspond, therefore, to access the most private zone, to control for the most public zone.

In this sense, privacy protects the confidentiality of communications from access to this information, as well as control, even after access has been designed.

1.3.2 Privacy as negative freedom

In this condition is body privacy. Close to access, or restriction (as negative freedom) to access. It deals with the right to deny that another person has access to the physical body, to touch it, or to restrict movement.

Similarly, the other types in the horizontal line of negative freedoms deal with the exclusion of access to control from others beyond the body, to the house (or other private space), to thoughts and property.

Thus, spatial privacy restricts the access of other people to that space considered private, such as the house, as well as to the intimate relationships of

family life that one has in this place.

While communication privacy restricts access to communications or controls the use of communications by third parties. In this sense, it covers much more than the access (extreme left, top, in the chart) of matches, but reaches, at another level, the control (lower right, in the chart) of the freely provided data.

In turn, proprietary privacy refers to a person's interest in using their property as a way to protect their activities, facts, things, or information from others. Like the one who keeps inside his own bag an object that he/she would not want to be seen by others, even if in a public space.

1.3.3 Privacy as positive freedom

As a right of positive freedom, privacy is classified, according to the authors, in intellectual, decisional, associational, and behavioral.

The first one is about the interest in thinking and in the development of opinions freely. It is declined to the left side of the table, in the most private sphere, because it is understood that thoughts are what we have most intimate.

While decisional privacy corresponds to choices drawn in intimate life, especially those focused on sexuality and procreation. Decisions about whether or not to have children, what kind of relationship to have with your partner or family members, are examples.

Associational privacy, in turn, is the free choice of whom to interact with: friends, groups, communities, or associations. It is in the category of semi-private because it compromises other people beyond the inner circle but is not yet in the totally public sphere.

And finally, behavioral privacy refers to publicly visible activities. As an ideal type of privacy, it has difficult application. It can be achieved only if "others" do not observe a certain behavior that occurs before the public. It can be glimpsed, for example, through surveillance cameras. The way to exercise freedom in such a situation would be an attempt to remain imperceptible among the masses.

In this sense, privacy protects the confidentiality of communications from access to this information, as well as control, even after access has been granted.

1.3.4 Informational privacy

Finally, informational privacy is distinguished from the other, but overlaps them, because it has an abstract character. It is related to each of the other types as their non-physical manifestation.

For example, while body privacy, not only physical access to the body should be protected, but also information related to it, such as genetics or a state of health.

Thus, privacy not only protects the body, space, communications, or behaviors, but also directly protects information about them. Although, by protecting such information, it often enters the "physical" territory of protection.

It belongs, at the same time, to the negative and positive aspects of freedom. It can be the deletion of information from a database or self-determination against the limits of analysis of the database, for example.

The typology presented will guide the understanding of the application of the right to privacy for the other chapters of the thesis. Thus, it is important to clarify that data protection is not synonymous with the right to privacy, as will be deepened in Chapter 2.

1.3.5 Typology applied to Brazilian legislation

The protection of the right to privacy takes the same breadth of meanings as the right it upholds. Therefore, it would be unlikely to accurately redeem all the legal instruments that somehow uphold such a right.

The Constitution of the Federative Republic of Brazil, of 1988, does not use the term "privacidade", but holds the meanings explored here in other

expressions, such as "private life", "intimacy", "secrecy" and "inviolability"[99].

At the infra-constitutional level, the Civil Code protects some types of privacy rights as personality rights and is therefore non-transferable and indispensable[100]. It deals, for example, with the disposition of the body itself, including for the purpose of organ transplantation, medical treatment, or surgical intervention.

It also ensures that the individual's name is not used, without authorization, for commercial purposes. It also restricts "the dissemination of writings, the transmission of the word, or the publication, exposure or use of a person's image", and may be prohibited "if they achieve honour, the good fame or the respectability, or if they are intended for commercial purposes"[101].

---

[99] Art. 5º, X – the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured;
Art. 5º, LX – the law may only restrict the publicity of procedural acts when the defense of privacy or the social interest require it;
Art. 5º, XII - – the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts;
At. 5º, XIV - access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity;
Art. 5º, XXXIII - all persons have the right to receive, from the public agencies, information of private interest to such persons, or of collective or general interest, which shall be provided within the period established by law, subject to liability, except for the information whose secrecy is essential to the security of society and of the State;
Art 5º, XXXVIII – the institution of the jury is recognized, according to the organization which the law shall establish, and the following are ensured: b) secrecy of voting;
art. 5º, LXXII - LXXII – habeas data shall be granted: b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative;
Art. 93, IX all judgements of the bodies of the Judicial Power shall be public, and all decisions shall be justified, under penalty of nullity, but the law may limit attendance, in given acts, to the interested parties and to their lawyers, or only to the latter, whenever preservation of the right to privacy of the party interested in confidentiality will not harm the right of the public interest to information;
Art. 136. Paragraph 1. The decree instituting the state of defense shall determine the period of its duration, shall specify the areas to be encompassed and shall indicate, within the terms and limitations of the law, the coercive measures to be in force from among the following: I – restrictions to the rights of: (...); b) secrecy of correspondence; c) secrecy of telegraph and telephone communication;
Art. 139. During the period in which the state of siege decreed under article 137, I, is in force, only the following measures may be taken against persons III - restrictions regarding the inviolability of correspondence, the secrecy of communications, the rendering of information and the freedom of press, radio broadcasting and television, as established by law;
[100] BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. **Código Civil.** Chapter II. Arts. 11-21.
[101] Art. 20. Unless authorized, or if necessary to the administration of justice or the maintenance of public order, the disclosure of writings, the transmission of the word, or the publication, the exhibition or use of the image of a person may be prohibited, to their application and without prejudice to the

Like the Constitution, the Civil Code contemplates "private life" as inviolable, in Article 21, providing for measures to prevent or terminate an act contrary to the norm.

Informational privacy is also protected in Brazilian law, in specific rules, regarding the confidentiality of tax agents[102], regarding telephone interception,[103] and the secrecy of banking operations[104].

Furthermore, the Consumer Protection Code[105], in addition to including consumer protection against abusive advertising[106], which already covers the use or capture of data that goes beyond the principles of information and objective good faith, is still dedicated specifically to databases, records, or records held by suppliers[107], with rules of civil law, procedural and criminal proceedings.

The Marco Civil of the Internet[108] sought to contemplate the right to privacy, mainly through the advent of new technologies with express protection[109]. But also, and not least, some of its different "types" implicitly manifested through the freedom of " guarantee of freedom of speech, communication, action and expression of thought (...)", "protection of personal data (...), and "preservation and guarantee of network neutrality"[110].

It also brought, related to the use of the Internet, the rights to "inviolability of intimacy and private life, its protection and indemnification for material or moral

---

indemnity, if they reach the honour, the good fame or the respectability, or if they are intended for commercial purposes.

[102] BRASIL. Lei. Nº 5.172, de 25 de outubro de 1966. **Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.** Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.

[103] BRASIL. Lei nº 9.296/1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.**

[104] BRASIL. Lei complementar nº 105, de 10 de janeiro de 2001. **Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências**.

[105] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de defesa do consumidor** (CDC).

[106] Art. 6º, IV; Art. 36; Art. 37.

[107] Art. 72.

[108] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet** (MCI).

[109] Art. 3º, inc. II.

[110] Art. 3, inc. I, III and IV.

damage arising from its violation", to the "inviolability of intimacy and private life, safeguarded the right for protection and compensation for material or moral damages resulting from their breach", "inviolability and secrecy of the flow of users' communications through the Internet, except by court order, as provided by law" and also the "inviolability and confidentiality of its stored private communications, except by court order"[111].

As for the collection, use, storage, and processing of users' data, it determines that they are constantly in the contract in a clear and complete way. And also there is no provision without consent to third parties of personal data (even if it does not limit what the personal or impersonal data would be)[112].

The framework also provides the guarantee of the right to privacy and freedom of expression in communications as a "condition for the full exercise of the right to access to the Internet"[113], and dedicates section II to the protection of records, personal data, and private communications.

And, of course, as the object of analysis of this research, the latest Brazilian data protection legislation, the General Data Protection Law[114], which will be addressed in more detail in the following chapters, aims to "protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person"[115]. It also brings privacy as the basis of the norm[116] and rights of the holder[117].

As seen, privacy is the physical condition of being isolated, and incarcerated. It is also the control of intimacy. And it can also correspond to the secret or determination of what information can be disseminated and which ones can't.

Other meanings were being embraced by the right to privacy. Sometimes

---

[111] Art. 7, inc. I, II and III.
[112] Art. 7º VI, VII e VIII.
[113] Art. 8º.
[114] BRAZIL. Law No. 13,709 of August 14, 2018. **General Law on the Protection of Personal Data** (LGPD). Wording given by Law No. 13,853, 2019. Brasília, DF: Senado Federal, 2018, art. 1º, griffin nosso.
[115] Art. 1º.
[116] Art. 2º, I
[117] Art. 17.

the concepts given are so broad that they do not corroborate the application of the law. On the other hand, so restricted that they do not incorporate the necessary protection. Furthermore, the problem is closely conditioned by the state of technology at a given time and society[118].

Brazilian doctrine uses several terms to represent it, which are also found in the legislation: private life, secrecy, intimacy, reservation, etc. Similarly, American doctrine uses the key term "privacy" to represent different types of rights.

Thus, the specific objective of this chapter is fulfilled to the delimitation of what represents the right to privacy, bringing its multiple meanings as a basis of understanding to the next chapters.

[118] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

CHAPTER 2

DATA PROTECTION

2.1 Delimitation of the right to data protection

Whether in the physical or digital world, human presence always leaves traces. Upon entering a place, it is contaminated with marks, footprints, and remains of body tissues. In the same way that something from that environment is taken away.

The digital traces, likewise, represent all the traces that remain on the human presence in virtual space. What was searched, the order in which it was searched, the time of use for reading a particular page, the time of use, the geolocation and so many other infinite information possible to be created from the combination of these tracks.

Digital footprinting is harvested in real-time whether in the use of applications, social networks, browsers or, simply because someone is carrying an electronic device, even without any interaction with it.

The experience of using the internet is certainly improved by prior knowledge of the user's expectations. The use of "cookies"[119], for example, makes it possible to make an online purchase, insert products in the shopping cart and continue browsing for new products without eliminating the previous choice. It is thanks to the storage of information that the choice of the first product will not be erased when the screen is closed from payment to return to search.

As well as the recall of passwords, or registrations on websites *after logging in with the information previously filled* in as the delivery address, or other

---

[119]"A "cookie," then, is the piece of information that the server and client pass back and forth. The amount of information is usually small, and its content is at the discretion of the server. In general simply examining a cookie's value will not reveal what the cookie is for or what the value represents." KRISTOL, David. M. HTTP Cookies: standards, privacy, and politics. **ACM Transactions on Internet Technology**, Vol. 1, #2, November 2001 Available at: <https://doi.org/10.48550/arXiv.cs/0105018> Accessed 29 Aug., 2022.

usage patterns that may bring convenience to the user.

Collecting, storing, and processing data is an essential activity for the use of technology today. No social network would have usability without the connection between the identity of the person using it and their friends, for example.

In this sense, digital traces are classified as active footprinting or passive footprinting. The actives are all information left by the user voluntarily when using a particular tool. Be directly, such as sending emails, visiting websites, filling out forms, posting photos, etc; or indirectly by "tagging" others about published content. All these traces come from the action of users in the use of the Internet[120].

On the other hand, traces left passively are data collected unintentionally and without the user's clear knowledge. As an example, browsing search engines become more intuitive and effective if they can assume from a behavior profile, what the person would expect to find. Thus, research coming from a connection in Brazilian territory would favor results from the same locality. It is possible to contextualize the research proposed by the algorithms previously collected from the user, even if the user does not know or does not notice the connection between his previous activity and future reflexes.

> the consequences of posting information on social networks can be unpredictable: only 70% of the information remains under the control of the user, and 30% of actions are not subject to control by the users themselves and can be used by unauthorized persons or intruders, including to commit illegal acts[121].

By reexploring the positive and negative contours arising from the practice, it is possible to point out the fight against internet fraud by security instruments that act in the crossing of data as an extreme, and the exploitation of the user's vulnerability in the other. Thus, the user who makes a credit card purchase, for

---

[120] OLINDER, Nina; TSVETKOV, Alexey; FEDYAKIN, Konstantin; ZABURDAEVA, Kristina. Using digital footprints in social research: an interdisciplinary approach. **Wisdom** 3(16), 2020, p. 127. Available at: <https://cyberleninka.ru/article/n/using-digital-footprints-in-social-research-an-interdisciplinary-approach/viewer> Accessed in 31 Aug., 2022.

[121] OLINDER, Nina; TSVETKOV, Alexey; FEDYAKIN, Konstantin; ZABURDAEVA, Kristina. Using digital footprints in social research: an interdisciplinary approach. **Wisdom** 3(16), 2020, p. 127. Available at: <https://cyberleninka.ru/article/n/using-digital-footprints-in-social-research-an-interdisciplinary-approach/viewer> Accessed in 31 Aug., 2022.

example, when returning to use the same card may have their identity proven. Similarly, the use of this initial information of data on the card can be fraudulently attacked with the "theft" of that identity. Therefore, the same information collected that protects, may be the same as that exposed to danger.

In a thinner line, which is the object of this work, is the user's tracking to collect their habits for the commercial purpose of monetizing the data. A topic that will be addressed in its relation to childhood in the next chapter.

It is important, however, to delimit that when using the term "data protection", the rights protected are broadly covered. It is not only the right to privacy, but also the right to access to information, the right to health, and the right not to be discriminated against, within other possibilities that will be addressed individually.

2.1.1 Data privacy, data security, and data protection

There is confusion, especially in Portuguese language doctrine, regarding the terms "data privacy", "data security" and "data protection". Methodologically it is necessary, then, to address the differences and how the expressions can be interpreted in the content of this thesis.

Data privacy requires that data be kept secure, but data may be kept secure for reasons other than privacy[122]. The conflation of privacy and security arises from the mistaken impression that data privacy is about keeping data private.

> If data privacy is viewed as the power to keep data secluded and safe from view, then data privacy and data security are the same. This conflation turns, however, on the mistaken view that data privacy is purely about concealment. This is only partially true. In all contexts that matter, data privacy involves a bilateral or multilateral relationship between a discloser and a recipient, or recipients, of information. Privacy is not usually about data concealment, it is about enforcing norms and expectations concerning data sharing[123].

As previously seen, privacy is a broad term that covers different rights,

---

[122] SCHWARTZ, Paul. Privacy and Democracy in Cyberspace, 52 **VAND. L. REV**. 1609-1663, 2001

[123] JANGER, Edward. Locating the Regulation of Data Privacy and Data Security. **Brooklyn Journal of Corporate, Financial & Commercial Law**, vol. 5, no. 1, Fall 2010, p. 97-110. HeinOnline, p. 99.

especially by American interpretation.

> the right to privacy was or is evoked to regulate, among others, tranquility in the home itself, control over personal information, control over the body itself, freedom of thought, control over surveillance, protection of reputation, protection against abusive investigations and interrogations, family planning, the education of children themselves, abortion, euthanasia, among others (free translation)[124][125].

Through the typology presented, it was found that informational privacy is present in every aspect as the other side of the coin. For each right protected, there is also information that can be violated. However, privacy is much more comprehensive because it is not necessarily data as seen. Privacy also protects the body, space, and physical communications or behaviors; regardless of the information behind it.

The object of the protection of privacy is the feeling, hardly captable and subjectively delimited. Data protection, on the other hand, is not limited to ensuring privacy, although this is one of the main goals. However, protection and control, monitoring, and supervision become objectively more concrete.

Regulating data protection is, in short, raising the right to privacy to the level of objectivity, at least regarding information.

In English, there is a noticeably clear distinction between "data privacy" and "data protection". The first concerns data subjects' privacy protection issues, and the second concerns data security and integrity. That is, the first flexes to the user, and the second to the data.

In Portuguese this distinction also takes another question, that the term "data privacy" would not be appropriate, as the data are not right-holder, therefore have no right to privacy. The appropriate term would be "data protection".

Methodologically, the English forms of "data privacy" will be used to talk about the general aspects of protection of the individual and "data security" when

---

[124] The various examples of these applications can be found in the judicial debates listed in the first chapter.

[125] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 217.

relating to data integrity.

The term "data protection", on the other hand, will take a broad sense of protection to privacy and security. So, data protection melds the fields of data privacy: how to control the collection, use, and dissemination of personal information) and data security: how to protect personal information from unauthorized access or use and respond to such unauthorized access or use.

In a historical analysis, as will be seen below, many laws dealt with security and privacy in different standards. The latest legislation on the subject, however, tends to unify data-related issues under the optimal "data protection".

Having made this initial distinction, it is necessary to recognize the role of data protection as a construction of law.

2.1.2 Building the right to data protection: dignity versus liberty

The United States and the European Union present two models of the construction of the right to data protection with enormous influences on the solutions adopted in other legal systems. This topic is not intended to address in depth the differences and similarities between them, but to point out the basis of the fundamental right of dignity, which is based on the European model, and freedom, which underpins the American.

This division does not necessarily reflect between common law and civil law, as several countries that are part of common law, such as Australia, New Zealand, and Canada, have mixed characteristics in their data protection disciplines, often getting closer to elements of the European model, as well as the United Kingdom itself[126].

Data protection, when dealing with the privacy element, gains different legal perspectives depending on the implied value given to the right. Different

---

[126] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 186-187.

cultures value privacy differently and thus exert different influences on personal data protection regimes.

> So why do these sensibilities differ? Why is it that French people won't talk about their salaries, but will take off their bikini tops? Why is it that Americans comply with court discovery orders that open essentially all of their documents for inspection, but refuse to carry identity cards? Why is it that Europeans tolerate state meddling in their choice of baby names? Why is it that Americans submit to extensive credit reporting without rebelling? These are not questions we can answer by assuming that all human beings share the same raw intuitions about privacy. (…) We have intuitions that are shaped by the prevailing legal and social values of the societies in which we live. In particular, we have, if I may use a clumsy phrase, juridified intuitions-intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture[127].

Thus, the resistance of the United States to link the matter to fundamental rights or models such as the protection of dignity is clarified to the extent that there is an understanding of the difference between approaches. America is much more oriented toward the values of liberty[128].

A good example may be "free speech", as a constitutional guarantee provided for in the first amendment to the U.S. Constitution, which is elevated with greater consideration when confronted with privacy, under the same justification[129]:

> Privacy is not the only cherished American value. We also cherish information, and candour, and freedom of speech. We expect to be free to discover and discuss the secrets of our neighbors, celebrities, and public officials. We expect government to conduct its business publicly, even if that infringes the privacy of those caught up in the matter. Most of all, we expect the media to uncover the truth and report it not merely the truth about government and public affairs, but the truth about people. The law protects these expectations too-and when they collide with expectations of privacy, privacy almost always loses[130].

---

[127] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., p. 1160.

[128] Americans and Europeans certainly do sometimes arrive at the same conclusions. Nevertheless, they have different starting points and different ultimate understandings of what counts as a just society. If I may use a cosmological metaphor: American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity. There are certainly times when the two bodies of law approach each other more or less nearly. WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., p. 2004.

[129] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., 1196.

[130] ANDERSON, David A. The Failure of American Privacy Law, in **Protecting Privacy** 139. Basil S.

From this perspective, it is possible to better understand why the Supreme Court has interpreted the Constitution to provide individuals with a right to privacy, but this right generally guards only against government intrusions[131]. Above all, individual freedom is valued to elevate it to constitutional status.

Thus, data protection is not addressed at the constitutional level. Nor does the United States have a general data protection law at the federal level. It was left to Congress to enact a number of federal laws in the matter of protecting personal information. With different scopes, it takes a sectoral approach, for example:

- Children's Online Privacy Protection Act[132]: provides data protection requirements for children's information collected by online operators. This standard will be analyzed in greater depth in the next chapter;

- Communications Act of 1934[133]: includes data protection provisions for common carriers, cable operators, and satellite carriers;

- Computer Fraud and Abuse Act[134]: prohibits the unauthorized access of protected computers;

- Consumer Financial Protection Act: regulates unfair, deceptive, or abusive acts in connection with consumer financial products or services;

- Electronic Communications Privacy Act: prohibits the unauthorized access or interception of electronic communications in storage or transit;

- Fair Credit Reporting Act: covers the collection and use of data contained in consumer reports;

Markesinis ed., 1999, p. 140.

131 MULLIGAN, Stephen. **Data Protection and Privacy Law**: An Introduction. Congressional Research Service (CRS), 2019. Available at: <https://crsreports.congress.gov/product/pdf/lF/IF11207> Accessed 01 Mar., 2022.

132 15 U.S.C. §§ 6501-6506 (2018). **Children's Online Privacy Protection Act of 1998**. Available at: <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim#sourcecredit> Accessed 01 Mar., 2022.

133 47 U.S.C. § 151 et seq. **The Communications Act of 1934**. Available at: <https://www.law.cornell.edu/uscode/text/47/229> Accessed 01 Mar., 2022.

134 18 U.S.C. § 1030. **Computer Fraud & Abuse Act.** Available at: <https://www.law.cornell.edu/uscode/text/18/1030> Accessed 01 Mar., 2022.

- Federal Securities Laws: may require data security controls and data breach reporting responsibilities;
- Federal Trade Commission (FTC) Act: prohibits "unfair or deceptive acts or practices";
- Gramm-Leach-Bliley Act: regulates financial institutions' use of nonpublic personal information;
- Health Insurance Portability and Accountability Act: regulates health care providers' collection and disclosure of protected health information and
- Video Privacy Protection Act: provides privacy protections related to video rental and streaming.

It is necessary to consider that the construction of the right to privacy is a product of “local social anxieties and local ideals”.

> In the United States, those anxieties and ideals focus principally on the police and other officials, and around the ambition "to secure the blessings of liberty," while on the Continent they focus on the ambition to guarantee everyone's position in society, to guarantee everyone's "honor." This was already true in 1791, in the French Revolution of Jerôme Petion, and it remains true today[135].

From the European perspective, honor is the great guide value that elevates privacy to the status of a fundamental right, relating it to dignity[136].

This understanding is especially illuminating for understanding the scope of data protection in two cultures that value the same right but apply it for different purposes: the defense of freedom, or the defense of dignity.

There are also, disregarding countries that have only sectoral laws, one hundred and forty-three countries or territories with general data protection laws,

---

[135] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., p. 1219-1220.
[136] WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., p. 1160.

such as Brazil[137], through the General Data Protection Law.

Among them are several convergences beyond their peculiarities, which makes the theme even more challenging. In addition, data does not find physical boundaries between countries or continents. In a transnational society, where data flows (almost) freely, it is necessary to establish at least principles that shape dialogue between the parties: a common denominator of rights.

In this sense, chapter 4 will address transnational data protection principles.

2.1.3 Autonomous fundamental right

The intimate connection between privacy and data protection remains clear from the explanations brought so far in this work. In this chapter, it was also possible to differentiate the terminology used by legislation and doctrine by referring to data privacy, data security, and data protection. Next, it is going to be demonstrate the construction of the right to data protection from two distinct bases: protection of dignity and protection of freedom.

Finally, it is then necessary to fix the right to data protection in its autonomy of other rights (such as privacy itself), in the context of Brazilian law.

---

[137]Åland Islands, Albania, Algeria, Andorra, Angola, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, The Bahamas, Bahrain, Barbados, Belarus, Belgium, Benin, Bermuda, Bonair, Saint Eustatius and Saba, Bosnia and Herzegovina, Botswana, Brazil,British Virgin Islands, Bulgaria, Burkina Faso, Canada, Cape Verde, Cayman Islands, Chad, Chile, China, Colombia, Costa Rica, Croatia, Curacao, Cyprus, Czech Denmark, Republic, Dominican Republic, Ecuador, Egypt, Equatorial Guinea, Estonia, Faroe Islands, Finland, France, Gabon, Georgia, Germany, Ghana, Gibraltar, Greece, Greenland, Guernsey, Guinea, Hong Kong, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Ivory Coast, Jamaica, Japan, Jersey, Kazakhstan, Kenya, Kosovo, Kyrgyzstan, Latvia, Lebanon, Lesotho, Liechtenstein, Lithuania, Luxembourg, Macau, Madagascar, Malaysia, Mali, Malta, Mauritania, Maurgy, Mexico, Moldova, Monaco, Mongolia, Mongolia, Montenegro, Morocco, Nepal, The Netherlands, New Zealand, Nicaragua, Niger, Nigeria, Norway, Oman, Panama, Peru, Philippines, Poland, Portugal, Qatar, Republic of North Macedonia, Republic of Serbia, Republic of the Congo, Romania, Russia, Rwanda, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Sechelles, Singapore, Sint Maarten, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Tajikistan, Thailand, Togo, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Uganda, Ukraine, United Arab Emirates, United Kingdom, Uruguay, Uzbekistan, Zambia and Zimbabwe. IAPP. **Global Privacy Law and DPA Directory.** Available at: <https://iapp.org/resources/global-privacy-directory/> Accessed 01 Mar., 2022.

Until 2020 it was understood that the confidentiality of communications only deserved constitutional protection (with a fulcrum in Article 5, item XII, of the Constitution), based on the conception of the right to privacy as an individual guarantee of state abstention in the individual private sphere[138].

From the historical judgment of five Direct Actions of Unconstitutionality (ADIs n. 6387, 6388, 6389, 6393, 6390), which occurred on May 6 and 7, 2020, the Brazilian Supreme Court (STF), by a majority, it ordered the suspension of the effectiveness of Provisional Measure No. 954/2020 and affirmed the existence of a fundamental autonomous right to data protection.

The current and recent position surpassed the old jurisprudence[139] of the same court by highlighting the independence of the right to privacy and other individual freedoms to the right to the protection of personal data.

In doing so, the Supreme Court ended up also clearly distancing the right to privacy broadly for its restricted aspect within data protection.

In 2021, the Proposed Amendment to Constitution No. 17 of 2019 was approved, which amended Articles 5, XII, and 22, XXX, of the Federal Constitution to include the protection of personal data as a fundamental right and establish the union's private competence to legislate on the subject, with the following text:

> Art. 5º (...) XII - the secrecy of correspondence and of telegraphic, **data,** and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts;
>
> Art. 22 The Union has the exclusive power to legislate on:
>
> XXVI - organize and supervise the protection and processing of personal data, in accordance with the law.
>
> XXX - protection and processing of personal data.

In practice, the recognition of the right to data protection as a fundamental right gives it autonomy of the right to privacy, as well as other fundamental rights such as life, dignity or freedom.

---

[138] RE 418.416, Tribunal Pleno, julg. em 10/5/2006, public. em 19/12/2006 no DJU.
[139] RE 418.416, Tribunal Pleno, julg. em 10/5/2006, public. em 19/12/2006 no DJU

2.2 What's at risk

Thus, based on the understanding that informational privacy derived from data protection is a vertex of the right to privacy, this chapter will also seek to guide what is at risk when processing[140] this information.

2.2.1 The value of personal information

The value of personal information will be classified as a risk for exponentiating all the others. The contemporary importance of personal information, both for the use of marketing and ideological strategies, increases the risk when processing these data.

Information is a central role in contemporary society. It is from and around it that society organizes itself. The increasing possibility of access to information, given by technology, has propelled us to another level of storage. However, what characterizes the real revolution is the application of the knowledge generated from the treatment of this information, in a cumulative feedback cycle[141].

The consumer, who was once merely the recipient of sales strategies, became the asset itself from his personal information.

It was from the possibility of organizing them in a more scalable way, from Big Data, that it became possible to sustain a new market model, in which every casual click, like or search is claimed as an asset to be tracked and monetized by someone.

The information produced by the data subject assists in the production process that is modeled according to the generated models. If before, the ads in

---

[140] Data processing for this work will have broad meaning, as the LGPD defined in art. 5, inc. X - processing: every operation performed with personal data, such as those related to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, modification, communication, transfer, dissemination or extraction.

[141] CASTELLS, Manuel. **Rise of the newwork society**: the information age: economy, society and culture. Vol. I, second ed. 2009, p. 69

magazines, newspapers and television the consumer was only a mass, a collectivity, without individualized characteristics, now it is possible to understand infinite possibilities of combinations of desires, emotions, and wills that lead to strategies surgically applied to each.

Advertising has become increasingly targeted, accurate, and profitable. Personal data has become the economic cog of this new society.

> In this new logic, human experience is subjugated to surveillance capitalism's market mechanisms and reborn as "behavior." These behaviors are rendered into data, ready to take their place in a numberless queue that feeds the machines for fabrication into predictions and eventual exchange in the new behavioral futures markets[142].

This commodification of behavior from the capitalism of surveillance is made in an unclear, indecipherable, and expert way. It appears to the data subject that the processing of your information is for your own benefit, through the personalization of your access to that product or service. However, parallel operations with this same information are the real business that converts into sales and strategies beyond the user's interest, without the user having any control[143].

In this way, (…) "we are exiles from our own behavior, denied access to or control over knowledge derived from its dispossession by others for others"[144]. For this new form of surveillance organization, people are merely "natural resources"[145] to the process. The value is not in the human, but in its data. The citizen becomes a mere spectator of his information.

Through smartphones people are increasingly connected, generating more and more data about every detail of their daily life. And through this, geolocation becomes an example of a powerful marketing resource, and a novelty in this area of advertising, in which the consumer is not aware of the provision of their

---

[142] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019, p. 100.
[143] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019.
[144] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019, p. 100.
[145] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019, p. 100.

data for purpose that is has been collected.

Billboards around the city could, in a way, induce consumption in a certain locality. However, geolocation reaches a new level. It is possible to advertise to those near the consumption area with a profile compatible with that product or service.

> A marker for mobile e-commerce ('mcommerce') is developing in which location data is crucial. Location data is typically sold by the telco originally collecting the data to third parties who ten in their turn use it to sell services to mobile users on a basis location or proximity, eg taxis, nearest fast foods, weather forecasts (...)[146].

It makes sense, then, the purchase of Waze by Google, for the value of US$ 1.3 billion[147]. The richness of the "free" app is exactly in the data it generates for this rich market.

Emotions, previously restricted to intimacy, have also gained a new level of possibilities for analysis and consequent generation of personal data. Companies like Microsoft, Apple and Google have invested in this area to:

> (i) the patenting of emotion-based ad targeting technology;
>
> (ii) the implementation of a motion processing system (M7), which identifies the displacements of users to specify their mental state at the time of interaction with the cellphone;
>
> (iii) projection of a system to detect smiles and other facial expressions of those who watch videos on YouTube[148].

From this movement of companies in capturing, interpreting and using feelings for the logic of marketing science, personal information is gaining more and more commercial value.

Surveillance finds no borders, and personal information is increasingly detailed and therefore valuable, basing a whole business model on which "free" services are paid at high costs of privacy violation.

---

[146] EDWARDS, Lilian; HATCHER, Jordan. Consumer privacy law 2: data collection, profiling and targeting. In: EDWARDS, Lilian; WAELDE, Charlotte (Coord.). **Law and the internet**. Portland: Har Publishing, 2009. p. 516-517

[147] COHAN, Peter. Four Reasons Google Bought Waze. **Forbes**. Available at: <https://www.forbes.com/sites/petercohan/2013/06/11/four-reasons-for-google-to-buy-waze/?sh=1109838f726f> Accessed 08 Set., 2020.

[148] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 46.

2.2.2 The discrimination of algorithm models

Algorithms can be defined as “systematic procedure that produces—in a finite number of steps—the answer to a question or the solution of a problem”[149]. An algorithm does not necessarily represent a computer program, but rather the steps required to accomplish a task.

They are typically used to perforate calculations, data processing, automates reasoning, automated decision-making among other tasks.

They are, then, the algorithms that take the information out of a cluster of unimportant data, to transform it into powerful instruments of new and specific possible interpretations. Big Data has a power of prediction, from past data, invaluable for marketing purposes.

In addition to the privacy problem with the intense increase in the behavior of data subjects in the use of their mobile phones and internet, and the massive analysis of this information; algorithms take us to another level: decision-making.

> In many states, algorithms based on what is called machine learning are also used to inform bail, parole, and criminal sentencing decisions. Algorithms are used to deploy police officers across cities. They are being used to make decisions in all sorts of domains that have direct and real impact on people’s lives. All this raises questions not only of privacy but also of fairness, as well as a variety of other basic social values including safety, transparency, accountability, and even morality[150].

Important decisions that affect people's lives are made every day from a model processed by algorithms that raise issues that include the limits of use, the necessary regulations and how to ensure, in fact, the enforcement of situations that are often "secret".

These decisions made by machines, called machine learning, without human intervention, “are often so complex and opaque that even their designers

---

[149] BRITANNICA. **Algorithm**. Available at: <https://www.britannica.com/science/algorithm> Accessed 03 Set., 2021.
[150] KEARNS, Michael; ROTH, Aaron. **The ethical algorithm**: the science of socially aware algorithm design. NEW YORK: Oxford University Press, 2019, p. 3

cannot anticipate how they will behave in many situations”[151].

Author of the book Weapons of Math Destruction, O'Neil argues that algorithms generate injustice because they are based on mathematical models created to reproduce human prejudices, misconceptions, and biases, in a discriminatory spiral, as follows:

> poor people are more likely to have bad credit and live in high-crime neighborhoods, surrounded by other poor people. Once the dark universe of WMDs digests that data, it showers them with predatory ads for subprime loans or for-profit schools. It sends more police to arrest them, and when they’re convicted it sentences them to longer terms. This data feeds into other WMDs, which score the same people as high risks or easy targets and proceed to block them from jobs, while jacking up their rates for mortgages, car loans, and every kind of insurance imaginable. This drives their credit rating down further, creating nothing less than a death spiral of modeling. Being poor in a world of WMDs is getting more and more dangerous and expensive[152].

According to the author, to build an algorithm it takes two things: a database of information about the past and a definition about "success": what is sought or expected with that analysis. It is in this second aspect that the reproduction of prejudices is evidenced. They are human beings, embedded in beliefs and limitations that program machines from their personal convictions, or professionals about success.

To understand the dynamics of algorithmic oppression one must overcome the idea of them being benign, neutral or objective, as they are not. The mathematical formulation that guides the decisions of algorithms are made by human. And like every human being, they carry “values, many of which openly promote racism, sexism, and false notions of meritocracy, which is well documented in studies of Silicon Valley and other tech corridors”[153].

Still, classifications are generated by secret formulas that, most of the time, are not intelligible to those who are being evaluated and do not provide for any

---

[151] KEARNS, Michael; ROTH, Aaron. **The ethical algorithm**: the science of socially aware algorithm design. NEW YORK: Oxford University Press, 2019, p. 7.
[152] O’NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 165.
[153] NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. New York: New York University Press, 2018, p. 2..

system of complaint to decisions. Sometimes they are covered up by the "industrial secret", crucial to business. Defended as intellectual property of companies, “in the case of web giants like Google, Amazon, and Facebook, these precisely tailored algorithms alone are worth hundreds of billions of dollars”[154].

The reason, as already specified in the previous topic, is the value of personal information for business models based on the economy of information from the processing of personal data.

2.2.3 The guarantee of "free consent"

Consent is one of the mechanisms by which legal acts are constituted. In relation to data protection, it gains even greater dimension because it is the primary basis of the legality of data processing, in most cases.

In this sense, “consent is a “fundamental legal instrument for transforming unlawful conduct into lawful conduct”[155]. Whether or not to consent on a particular subject, the individual would exercise his freedom and self-determination.

The understanding behind this notion is that data subjects would be able to make conscious, rational, and autonomous choices about their data. Esse pressuposto combina com o papel de protagonista fundado no direito do indivíduo de controlar os seus dados pessoais, expresso, principalmente, a partir da segunda geração de leis de proteção de dados[156].

Both the GDPR[157] and the LGPD[158] treat consent as informed, free,

---

[154] O’NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016, p. 30.
[155] VAN DER HOF, Simone. Agree... Or do I?: a rights-based analysis of the law on children’s consent in the digital world. **Wisconsin International Law Journal**, vol. 34, p. 101-136, 2016, p. 1.
[156] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 188.
[157] Art. 4, (11) consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
[158] Art, 5, XII - consent: free, informed and unambiguous manifestation by which the holder agrees to the processing of his personal data for a specific purpose;

express, specific, or unambiguous: placing it at a level that makes it believe that there is an autonomy of the will of the data subject[159].

> Thus, there is a regulatory framework encapsulated by a reductionist understanding of the content to which informational self-determination should be referred to, which, after more than two decades, no longer fits the underlying context of personal data as an economic asset in constant circulation (...) and that modulates the free development of the personality of citizens (...) (free translation)[160].

On the other hand, there is growing doubt about the effectiveness and even the fairness of consent in the context of data processing[161]. Although control is a necessary component to any regulation on the subject, control over the data is not obtained from consent, as expected[162].

The reasons for this are broad, and it resides from the way this consent is requested to particular conditions of how it is expressed.

Primary, cognitive ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data, are extremely limited[163]. The complex legal terms and amount of detail make it difficult for those who try to find out about the privacy policy clauses.

> Second, and more troubling, even well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems. There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. Moreover, many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses, further limiting the effectiveness of the privacy

---

159 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 188.
160 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 188.
161 SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. The Crisis of Consent: fow stronger legal protection may lead to weaker consent in data protection. **16 Ethics & Info**. Tech. 171, 2014
162 SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.
163 SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903, p. 1881-1882.

self-management framework[164].

In addition, users are constantly plagued with notifications to consent to any action, and do so that it is possible to move on to the next step: entry on the site, purchase of a product, access to information, etc.

Another problem is the impossibility, in some cases, of non-consent. Consent ends up being a conditional so that the user can have access to a product or service[165]. If there is no alternative consent is a fallacy. The user, within the data processing industry, does not have any real bargaining power over their data, and the control over them in this sense is little and dubious.

Thus, consent should be viewed with suspicion, and alternative practices will be suggested in the final chapter of the thesis.

2.2.4 Data breach

The theme of data breach approaches the terminology of "data security" more than "data protection" because it relates to information security, not specific user protection.

That is, data breach is a weakness in the storage security of this information that, consequently may or may not affect the protection of the user who has had their data exposed.

The central question of the breach is no longer whether or not the data will leak, but when it will happen, such are the possibilities of breaking safety standards, however sophisticated at that time may seem. The technology in its dynamism makes obsolete with great speed even extremely rigid controls.

Still, a large portion of companies that handle data use poorly secured

---

[164] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903, p. 1882.
[165] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1898.

databases, making it common the large-scale leaking of records[166].

The reason behind the carelessness of personal data, is the difficulty of the courts to identify the harm in situations of data breaches, causing companies to leave lawsuits unharmed, most times[167].

Data leakage can expose users' informational privacy in a vast and permanent way. Information that should be private, when made public, will never go back to the previous status.

“Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage”[168]. The problems can be of various orders, from the need for good credit for buying a property to even the search for a job; that can be threatened by the leakage of data that should be confidential.

Although these leaked data are still under theoretical protection of data laws, including the illicit use by a third party who does not have consent or who uses it outside the given purpose; the difficulty of tracking such situations is immense and the damage to the data subject can hardly be repaired.

Furthermore “they face an increased chance of being preyed upon by blackmailers, extortionists, and fraudsters promising quick fixes in exchange for data or money” [169]. The moral shock of the data leakage is still difficult to be proven in court because it contains an extremely subjective parameter in a diffuse situation of damage.

Large data leaks are shocked by the breadth of data and the number of victims, in increasing numbers.

Data breaches in 2021 set a new record with 5.9 billion accounts affected,

---

[166] NEWMAN, Lily Hay. If You Want to Stop Big Data Breaches, Start with Databases. **WIRED** (Mar. 29, 2017), https://www.wired.com/2017/03/want-stop-big-data-breaches-startdatabases/

[167] “Looking across the body of jurisprudence of data-breach harms, it is fair to say that courts are reluctant to recognize data-breach harms”. SOLOVE, Daniel; KEATS CITRON, Danielle. Risk and Anxiety: a theory of data-breach harms. **Texas Law Review**, vol. 96, no. 4, March 2018, p. 737-786, p. 785.

[168] SOLOVE, Daniel; KEATS CITRON, Danielle. Risk and Anxiety: a theory of data-breach harms. **Texas Law Review**, vol. 96, no. 4, March 2018, p. 745.

[169] SOLOVE, Daniel; KEATS CITRON, Danielle. Risk and Anxiety: a theory of data-breach harms. **Texas Law Review**, vol. 96, no. 4, March 2018, p. 745.

reported AtlasVPN[170]. Among these, 700 million LinkedIn users were affected and had their email addresses, full names, phone numbers, physical addresses, geolocation records, genders, personal and professional experience, and more, exposed. “LinkedIn noted that the data wasn’t acquired from an actual breach of its systems, but from “data scraping” of its internet-facing API”[171].

Facebook also had its data leaked. In April, information from 533 million users in 106 countries was scraped from Facebook and published on a hacking forum. It included phone numbers, full names, locations, email addresses, and users’ biographical information.

In the same month, but three years before, Mark Zuckerberg was called to testify before Congress, regarding the harvesting of the private data of over 87 million Facebook users by Cambridge Analytica, a company that pairs consumer data with voter information. In a Facebook post on March 21, 2018, acknowledging the massive security breach, Zuckerberg declared that “the good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there’s more to do, and we need to step up and do it”[172].

With the increasing leak since then, It seems that there is much more to be done.

In January 2021 there was also the exposure of the Chinese social media agency SocialArks, resulted in a data leak of 400 GB of personal data on about 214 million Facebook, Instagram, and LinkedIn users. The data included names, country of residence, contact information, the position of work, subscriber data, and profile

---

[170] MELLO Jr., John P. Data breaches affected nearly 6 billion accounts in 2021. **TechNewsWorld**. Jan 18, 2022. Available at: <https://www.technewsworld.com/story/data-breaches-affected-nearly-6-billion-accounts-in-2021-87392.html> Accessed 18 May, 2022.

[171] MELLO Jr., John P. Data breaches affected nearly 6 billion accounts in 2021. **TechNewsWorld**. Jan 18, 2022. Available at: <https://www.technewsworld.com/story/data-breaches-affected-nearly-6-billion-accounts-in-2021-87392.html> Accessed 18 May, 2022.

[172] SEGARRA, Lisa Marie. **Mark Zuckerberg Just Revealed 3 Steps Facebook Is Taking to Address the Cambridge Analytica Crisis Time**. March 21, 2018. Available at: <https://time.com/5209729/mark-zuckerberg-facebook-cambridge-analytica/#:~:text=The%20good%20news%20is%20that,step%20up%20and%20do%20it.%E2%80%9D> Accessed 18 May, 2022.

links.

In the same month, Brazilians discovered that data from 220 million users were available in a dark web forum, containing names, unique tax identifiers, facial images, addresses, phone numbers, email, credit score, salary, and other information.

As revealed by the newspaper Estado de São Paulo[173], among the data leaked are the information of the President of the Republic, Jair Bolsonaro, the former president of the House of Representatives, the former president of the Senate and the 11 ministers of the Brazilian Supreme Court (STF).

The list also contains information from 40 million companies and information on more than 104 million vehicles, containing chassis number, vehicle plate, municipality, color, model, year of manufacture, cylinders and even the type of fuel used. In total, it is estimated that the hacker has almost 1 TB of data, 16 GB of them of people's face photos – representing about 1.1 million images[174].

The information is really alarming and puts virtually all the data of the practical life of Brazilians exposed. Thus, increasing the risks of misuse, exposure to privacy, virtual crimes, etc.

However, it is important to highlight that the risk of data leakage is not restricted to sensitive data, which clearly raise the level of damage, or to personnel. Even anonymized data poses risks, as you will see below.

2.2.5 The false anonymization of information

The laws of protection of personal data have as their exclusive object the

---

[173] ROMANI, Bruno. **Vazamento de dados**: Informações de Bolsonaro e ministros do STF estão à venda na internet. Estadão. Available at: <https://link.estadao.com.br/noticias/cultura-digital,dados-de-bolsonaro-e-ministros-do-stf-estao-a-venda-na-internet-apos-megavazamento,70003600653> Accessed 18 May, 2022.

[174] ROMANI, Bruno. **Vazamento de dados**: Informações de Bolsonaro e ministros do STF estão à venda na internet. Estadão. Available at: <https://link.estadao.com.br/noticias/cultura-digital,dados-de-bolsonaro-e-ministros-do-stf-estao-a-venda-na-internet-apos-megavazamento,70003600653> Accessed 18 May, 2022.

data that is personal, as the name suggests. Thus, anonymized data are outside the regulatory scope.

The anonymized data, in accordance with Article 5, III of the General Data Protection Law, is the “data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing”. Because they do not associate with a natural person, they are not subject to the restrictions brought by the LGPD, which allows greater freedom of treatment for this category.

However, no data is born completely anonymous. This makes it through technical means by which a data "loses the possibility of association, directly or indirectly, with an individual", and thus "also lose the 'power' of the application of the LGPD” (free translation)[175].

The data are anonymized when who collects it intends to use it for a different purpose for which it was originally consented. Through anonymization, these data are now subject to other uses, such as statistical use for any purpose.

However, the value of the data is in the knowledge obtained by the joint analysis of information, as evidenced by the algorithms. Find patterns and determine profiles by relating different points of data. Anonymization, on the contrary, unties this relationship between data so that it is not possible to identify specific people and their identities[176].

> This leaves those in charge of processing the data with a problem: how can they ensure that anonymization is conducted effectively on the data on their possession, while retaining that data's utility for potential future disclosure to, and further processing by, a third party?[177]

Another category brought by the GDPR[178] and integrated the LGPD is

---

[175] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019.
[176] STALLA-BOURDILLON, Sophie; KNIGHT, Alison Knight. Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. **Wisconsin International Law Journal**, vol. 34, no. 2, Winter 2016, p. 284-322. HeinOnline. p. 285.
[177] STALLA-BOURDILLON, Sophie; KNIGHT, Alison Knight. Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. **Wisconsin International Law Journal**, vol. 34, no. 2, Winter 2016, p. 284-322. HeinOnline. p. 285.
[178] ‘Pseudonymisation’ of data (defined in Article 4(5) GDPR) means “‘pseudonymisation’ means the

pseudonymization, being “the processing by means of which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment” (free translation)[179].

Thus, what differentiates an anonymous data from pseudoanonymous is that the second still contains the possibility of reassociation. Pseudonymization is therefore not a method of anonymization, but merely a method of data security. The controller keeps in a separate and controlled environment, additional information that puts again at the level of personal data covered by the LGPD, or the GDPR, for example.

The risk lies in false anonymization. That is, in the possibility of a data being classified as anonymous when in fact it is pseudoanonymous, in an attempt to circumvent the legal ties.

Or, in the ease of deanonymizing the information by the failure in the anonymization process. In addition to the removal of identifiers, the anonymization process should involve techniques that hinder a new identification, a process known as reidentification.

Anonymization is seen as a "silver-bullet" for privacy issues in the last forty years of data protection debates[180]. Ohm[181], calls it as “the release-and-forget”: an unfounded promise, since proven the limits of disindetification techniques by computer science.

In a more realistic assessment, the risks of reidentification are enormous. The author then recommends abandoning this distinction between personal data and

---

processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”

[179] Art. 13, § 4º

[180] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Vol. 57, p. 1701, 2010

[181] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Vol. 57, p. 1701, 2010

anonymized data[182].

Some cases of data leakage were emblematic in this aspect of the reidentification of supposedly anonymous data, leaving vulnerable those exposed.

One of the emblematic cases, also cited by Ohm[183] is the AOL Data Release, 2006. At the time, the company released a file with information from the surveys answered by more than 650,000 users of its search system. The disclosure of these data was intentional and for the purpose of serving as a database for various purposes, such as academic studies.

To try to maintain the anonymity of searches, login data has been replaced by unique identification numbers. The failure appeared in a few days, with several sites reporting the ease of reidentification of this information. The New York Times made a story in which was easily re-identified a person as Thelma Arnold "who acknowledged that she had authored the searches, including some mildly embarrassing queries such as 'numb fingers,' '60 single men,' and 'dog that urinates on everything'"[184].

This case ended up known as a major disaster in the corporate world and resulted in the resignation of those responsible for the idea[185].

That is, anonymization is not in fact a guarantee of data security and should be viewed with skepticism.

2.3 Why not protect? Arguments against data privacy protection

Although the risks presented are numerous, there is reluctance on the

---

[182] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Vol. 57, p. 1701, 2010, p. 1752.
[183] OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Vol. 57, p. 1701, 2010, p. 1718.
[184] BARBARO, Michael; ZELLER, Tom. A Face Is Exposed for AOL Searcher No. 4417749, **N.Y. TIMES**, Aug. 9, 2006, Available at: <https://www.nytimes.com/2006/08/09/technology/09aol.html> Accessed 13 Apr., 2020.
[185] ZELLER, Tom. AOL Executive Quits After Posting of Search Data, **N.Y. TIMES**, Aug. 22, 2006. Available at: <http://www.nytimes.com/2006/08/22/technology/22iht-aol.2558731.html> Accessed 13 Apr., 2020.

subject from some arguments contrary to data protection regulation. The last topic of the chapter will then address why not protect: arguments against data privacy protection.

2.3.1 The death of privacy

With so much technology that facilitates the dissemination of information from the "self" to the world, some wonder if the value of privacy in the digital age is still relevant. For many authors privacy would already be dead[186], either by the power of state surveillance, by the information society with its data-based economy or by the free exposure of personal information by the data subjects.

> We are living after the end of privacy. What it means to be human is changing because everything that can be seen and everything that can be put into words can now be instantly shared on screens the world over. We will need to invent social institutions that acknowledge the magnitude of this change and educational institutions that prepare people to live meaningful lives in the face of the superabundance of information. The clock is ticking. The cursor is blinking[187].

There are those, still, who consider privacy an overrated right, as Posner[188], which proves his theory from the fact that people would easily give up their privacy in exchange for very little, which would demonstrate the lack of interest in guardianship.

---

[186] Some books that are based on this idea: WHITAKER, Reg. **The End of Privacy**: How Total Surveillance Is Becoming a Reality. New Press, 2000; SYKES, Charles J. **The End of Privacy**: The Attack on Personal Rights at Home, at Work, On-Line, and in Court. St. Martin's Press, 1999; ROSENBERG, Jerry M. **The Death of Privacy**. Random House, 1969; WICKER, Stephen B. **Cellular Convergence and the Death of Privacy**. Oxford University Press, 2013; ANDREWS, Lori**. I Know Who You Are and I Saw What You Did**: Social Networks and the Death of Privacy. Free Press, 2012; GRAHAM SCOTT, Gini. **The Death of Privacy**: The Battle for Personal Privacy in the Courts, the Media, and Society. Changemakers Publishing, 2015; MILLER, Richard E. **On the End of Privacy**: Dissolving Boundaries in a Screen-Centric World (Composition, Literacy, and Culture). University of Pittsburgh Press, 2019; GARFINKER, Simson. Database Nation: **The Death of Privacy in the 21st Century**. O'Reilly Media, 2001.

[187] MILLER, Richard E. **On the End of Privacy**: Dissolving Boundaries in a Screen-Centric World (Composition, Literacy, and Culture). University of Pittsburgh Press, 2019, p. 233

[188] There's some moves to create new privacy rights, but it's overwhelmed by the convenience of surrendering your privacy. Ans it's a fact that people surrender it for other small gains is a sign them really, or most people really, value at that punch. Part because it's very much a relative kind of good. BIG THINK. **Judge Richard Posner:** privacy. Available at: <https://www.YouTube.com/watch?v=kQu0et1jXfs> Accessed 26 Jan., 2021.

The "death of privacy" is conditional on the morality of living significantly or not, about renouncing the sacred space of the private or arguments that will be exposed below, such as the "I have nothing to hide" or even the false trade-off between security or free services.

Privacy would be dead, in alarmist speeches, because people live an empty and shared life. Surely this discourse is worth more to psychology or sociology than to law. Regardless of motivations, whether good or bad, these are the contours of today's society.

This narrative can be disputed by the concept already brought about privacy: which is not only linked to secrecy, but also approaches the control of information, for example.

Privacy is not just about hiding something, it is also, and especially relevant today, by self-determination, autonomy and freedom. In this sense, in the computerized era and privacy exposure becomes probably one of the most important civil rights.

Another point of debate is the subjectivity of the exchange of "very little" for personal information. Sometimes accessing a website, providing credit card details or filling out a registration are the only way to access the product or service. Still, there is not always clarity of what is being given up when providing this information, which makes this discourse even more fragile[189].

2.3.2 "I have nothing to hide"

"I have nothing to hide", which gives title to the book of Solove[190], it concerns the common argument that "citizens of good" have nothing, or should not have, to hide, especially from the government. That is, that having lawful conduct, there would be no reason to seek privacy.

---

[189] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.
[190] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011.

A first counter-argument, supported by Miller[191], points out that “this incredibly insensitive attitude completely overlooks man’s need for individuality and ignores the variousness of the human condition”. It is not possible to reduce privacy to shame, or dishonor, as already seen.

Furthermore, Solove[192] treats it as "*all-or-nothing falacy*", that is, a fallacy that it is not possible to have privacy and security mutually and therefore one must give up privacy at the expense of security. The author rebuts by clarifying that “sacrificing privacy doesn’t automatically make us more secure” [193]. And yet that “not all security measures are invasive of privacy”[194].

This argument was popularly exposed after the revelations of Snowden [195] on U.S. government surveillance of its citizens and other countries. “Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”[196].

In very general terms, governments have an interest in security and stability that can sometimes actually overcome individuals' desires for some aspect of privacy. Companies, on the other hand, have only one final interest: making money.

When used for data control by companies, and in that case, in exchange for the convenience of receiving advertising or offers targeted only to your profile, would then be harmless surveillance?

Privacy is much more than protecting secrets. Privacy is power. How much power the government, or, in the case of the object of this thesis, a company, must

---

[191] MILLER, Arthur. **The assault on privacy**. Ann Arbor: University of Michigan, 1971, p. 63
[192] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011, p. 33-37.
[193] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011, p. 34.
[194] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011, p. 34.
[195] Sobre o caso: SCHEUERMAN, William E. Whistleblowing as civil disobedience: the case of Edward Snowden. **Philosophy & Social Criticism**, v. 40, n. 7, 2014, p. 609-628 e VERBLE, Joseph. The NSA and Edward Snowden: surveillance in the 21st century. **ACM SIGCAS Computers and Society**, v. 44, n. 3, 2014, p. 14-20.
[196] SNOWDEN, Edward. Edward Snowden: a right to privacy is the same as freedom of speech – video interview. **The Guardian.** Available at: https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video

have on someone's life. What could they do with your information? Even if the person is not doing anything wrong, they do not necessarily want to expose all their actions.

Of course, a search of the residence is legitimate when the possibility of threat by the state is proven. But to do so, there are objective criteria specified in law that must be observed. Every citizen has the right to know and understand such criteria to which is subjected.

It is no different for use by the private sector. Of course, some kind of collection is necessary: when we fill in our personal data, such as address, telephone number and identification documents, to buy an air ticket, for example. But this capture needs to be regulated. The citizen has the right to control the power, not only of the State, but also of companies, over his life. To this do so, it is primarily necessary to understand the criteria. Transparency in the capture and use of this information is required. And consent is required, because, unlike the State, there is no prior pact between the consumer and the company.

One of the points of defense in this argument is that the public security interest should always prevail in the "private" interest of privacy. However, Solove argues that privacy should be understood as a social value and therefore of public interest as well[197].

Thus, the balance between security and privacy is balanced on this criterion, and other factors of imbalance should be considered for concrete cases.

2.3.3 Privacy as opposed to the public interest

Privacy is often placed on the opposite side of the public, as in public versus private dialectics. However, as already demonstrated in the first chapter, there are many paths between the two extremes. Nuances of the expectation of access, confidentiality and control are part of this context.

The argument can also be contradicted from the perspective that privacy

---

[197] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011.

is not only an individual interest, but rather a "social value"[198], or even of collective interest.

> (...) a more accurate examination of the problem shows that certain characteristics of privacy can overcome this objection, which are its collective dimension (which involves, for example, the political connotation of control over the individual and the imperative of non-discrimination of minorities) and, more incisively, by the very interdependence of the protection of privacy with the free development of personality (free translation)[199].

Thus, there would be no opposition to the public interest, but, on the contrary, convergence. Bioni[200] presents data protection as an autonomous category of personality rights, breaking with the dichotomy of the public and private.

Even if the public is classified as publicity of something, in the same way there is no total divergence. “Privacy might not necessarily be opposed to publicity; its function might be to provide the individual with control over certain aspects of her life”[201].

In the taxonomy on privacy, presented Chapter 1, these nuances were well presented. There is a right to privacy even in the public sphere.

2.3.4 The false trade-off

It is very common to travel from the exchange of privacy to state security. Thus, people renounce a certain degree of their privacy so that the State can monitor, relate data, and use its intelligence to prevent, curb or investigate crimes such as terrorism, as already analyzed in the topic "I have nothing to hide".

However, another false trade-off is that related to theoretically free products and services offered on the internet. People are bombarded with extensive

---

[198] SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale university press, 2011.
[199] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 46.
[200]BIONI, Bruno Ricardo. **Protection of personal data**: the function and limits of consent. Rio de Janeiro: Forensics, 2019.
[201] INNESS, Julie. **Privacy, Intimacy, and Isolation**, New York and Oxford: Oxford University Press, 1992, p. 6.

requests for data collection that certainly do not correspond to the need for treatment for the purpose they are theoretically consenting to.

> Eventually, companies began to explain these violations as the necessary quid pro quo for "free" internet services. Privacy, they said, was the price one must pay for the abundant rewards of information, connection, and other digital goods when, where, and how you want them. These explanations distracted us from the sea change that would rewrite the rules of capitalism and the digital world[202].

And so surveillance capitalism emerges from the "logic of accumulation in which surveillance is a foundational mechanism in the transformation of investment into profit"[203]. With the promise of anticipating needs and making complex contemporary life into something simpler.

However, what you have in return is just the opposite. The bonds created by the ability to anticipate our thoughts and desires puts us in check our real autonomy in making decisions freely. Algorithms now play a crucial role for the human being: to decide.

The data are effectively what pays for online content. The problem with this bias is that people are not necessarily fully aware that they are paying it with their personal data, coming back again to the consent issue[204].

That is, it turns again to the question of consent as a tool that does not reach the full understanding and free will of those who sign it. In the case of free applications, the option is restricted to accepting and using the service or refusing and not using. There are no margins to negotiate. In the absence of an option, the user ends up consenting to the use of their data in a comprehensive way and often completely disproportionate to what they will receive in return, without having any idea of it. There is no trade-off.

Thus, Chapter 2 limited the right to data protection as a fundamental and autonomous right; addressed the risks involved and, to finally, bring the arguments

---

[202] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019, p. 55.
[203] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019, p. 55.
[204] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.

against the protection. Continuing, the next chapter will specifically focus on the theme of childhood and privacy and raise the sensitive points to this class of individuals.

CHAPTER 3
IMPACTS OF DATA COLLECTION IN CHILDHOOD AND REGULATION OF CHILDREN'S ADVERTISING

Chapter 1 has limited the scope of the right to privacy. From absolute secrecy to control in the public sphere, there is an informational vertex of privacy. And it is in this aspect that data protection is consolidated, as seen in Chapter 2.

Thus, by protecting data informational privacy is also protected. It remains for this chapter to address the privacy of data collection in childhood. Therefore, some methodological considerations are initially needed.

It is not the subject of this research to study privacy in the face of information held by the State for public policy purposes, for example, or by academic research entities, nor privacy outside the digital context.

Still, the proposed path will not be from the "moral panic" on the subject. That is, from the point of view of morality about the child exposing their data on the internet, or not. The construction of the text will be based on risks in order to seek ways that guarantee the right to privacy so that there is, consequently, the free development of personality and equal opportunities for children.

Children already make up one third of internet users in the world[205]. In Brazil, 82% of them access the network[206]. The experiments, discoveries, learnings, adventures typical of human development, correlate to the risks of exposing

---

[205] BYRNE, J., KARDEFELT-WINTHER, D., LIVINGSTONE, S., & Stoilova, M. (2016). **Global Kids Online Research Synthesis** (2015-2016). UNICEF Office of Research – Innocenti and London School of Economics and Political Science. Available at: <http://globalkidsonline.net/wp-content/uploads/2016/11/Synthesisreport_07-Nov-2016.pdf> Accessed 08 Jan., 2021.

[206] The proportion of network users was higher among the population aged 15 to 17 years (93%) and lower in the age groups 13 to 14 years (87%), 11 to 12 years (82%) and among those aged 9 to 10 years (74%). INTERNET MANAGEMENT COMMITTEE IN BRAZIL - CGI.br. **Research on the use of the Internet by children and adolescents in Brazil**: TIC kids online Brazil 2017. Survey on internet use by children in Brazil: ICT kids online Brazil 2017 [e-book] / Núcleo de Informação e Coordenação do Ponto BR, [editor]. -- São Paulo: Internet Steering Committee in Brazil, 2018. Available at: <https://cetic.br/media/docs/publicacoes/2/tic_kids_online_2017_livro_eletronico.pdf> Accessed 01/04/2019.

themselves to such.

It is also necessary to start from the understanding that children experience a special condition of development, different from those that produce the discourses of their protection. Take over the discourse of how the interaction of the child with technology should be is a risk of distancing from reality.

The method that seeks to investigate this research is an opposite reflection, of how technology should preserve the interests of the child, proposing, in the end, regulation of the use of the child's information, and not inhibitory measures for children.

Therefore, it is also important to finalize the chapter dealing with children's advertising regulations, since the data collected serve – in the end – as marketing strategies for profiling users as a target audience of advertising.

3.1 Childhood and vulnerability to the media

3.1.1 The effects of surveillance

The effect of surveillance on people's lives, in general, was portrayed by Bentham[207] on the prism of his theory of utilitarianism, by which the best actions and policies are those that lead to the best results to the greatest possible number of people, such as the Panopticon[208].

The Bentham Panopticon is a proposed prison model in which prisoners are arranged in cells around a central tower, so that there can be full vigilance over them, without the prisoners, however, being able to observe their observer. The idea is that the prisoner would not need to be watched all the time to behave as if he were, since he would have no control over this aspect.

When they are being watched, people behave in a more disciplined way,

---

[207] BENTHAM, Jeremy. **The panopticon**: or the inspection house. London: mews-gate, 1787.
[208] BENTHAM, Jeremy. **The panopticon**: or the inspection house. London: mews-gate, 1787.

which would be interesting “thus discipline produces subjected and practiced bodies, “docile” bodies. Discipline increases the forces of the body (in economic terms of utility) and diminishes these same forces (in political terms of obedience)”[209].

The idea of panopticon, in addition to the prison system, also has great reflections as a metaphor of electronic surveillance of today. Foucault developed the Panopticon theory by the aspect of “obtains power of mind over mind”[210], especially portraying how power is exercised by surveillance and creates a disciplined society.

That is, the population could be more easily shaped to the purposes of those who hold power when knowing that they are being watched and behaving to do so. This does not apply only to the control exercised by the power of the State. Through the prism of marketing, “the panopticon is a privileged place for experiments on men, and for analyzing with complete certainty the transformations that may be obtained from them”[211].

If on the one hand, who knows who is being watched shapes his behavior to suit the expectations of those who watches, the one who does not know is also the target of the Panopticon because it is even more susceptible to manipulation by power, after the identification of certain behavior profiles. Just as with capturing and using data for marketing purposes.

The powers of marketing over consumer decisions and behaviors has been widely explored in recent decades. However, it is the possibility of monitoring this consumer with great specificity that makes him especially vulnerable to panopticons.

In this context, privacy is not only a right of seclusion, but mainly of freedom. Freedom to think and behave freely from the shacks of continuous vigilance.

---

[209] FOULCAULT. Michel. **Discipline and punish**. New York: vintage, 1995. Surveiller et Pnir: Naissance de la prison. Paris: Gallimard, 1975, p. 138.
[210] FOULCAULT. Michel. **Discipline and punish**. New York: vintage, 1995. Surveiller et Pnir: Naissance de la prison. Paris: Gallimard, 1975.
[211] FOULCAULT. Michel. **Discipline and punish.** New York: vintage, 1995. Surveiller et Pnir: Naissance de la prison. Paris: Gallimard, 1975, p. 204.

Persons who hold public office are subject to having their salaries disclosed as a result of the transparency inherent in their position. People traveling through airports are subject to the search of their luggage and belongings. High-performance athletes are subject to anti-doping tests etc.

However, it cannot be said that the people mentioned above do not have the right to privacy. As already delimited in its own chapter, privacy reaches different dimensions of life and, in certain circumstances, this right may be restricted by another in some respect.

The analysis is made from the concrete case and in a very subjective way, since the idea of privacy is delimited from the immaterial goods of the human being and his right of personality.

In addition to the external limits to the exercise of privacy, as mentioned in the first chapter, there are still internal limits, in which each one establishes its barriers.

Privacy is a process in which the individual or groups negotiate their barriers, allowing the "other" to be within or outside these limits. Thus, these barriers between the "self" and the "other", can determine a physical contact or its repudiation, avoid being observed in a given situation, keep secret an idea or information about itself, among many other possibilities[212].

Therefore, the idea of privacy reflects human relationships and communication exchanges, establishing barriers between what is outside and what is within reach of the other. Thus, when communicating, a door opens to what is within the self and the opportunity of the other to take care of this intimate space.

Privacy, in this sense, is shaped from what the individual establishes as restricted access of his being. If today it is not relevant for a particular person to restrict access to their photograph exposed on a social network, it does not mean that that same person is renouncing all the limits of their privacy. Nor does it mean that, at another time in your life, that same photograph will be part of your restricted

---

[212] These ideas have already been explored in the first chapter.

universe.

Privacy is also a social construct, and it differs from expectation about what should be private in different cultures or groups.

> Privacy is a difficult notion to define in part because rituals of association and disassociation are culturally relative. For example, opening a door without knocking might be considered a serious privacy violation in one culture and yet permitted in another[213].

Just as the concept of privacy gains larger and smaller dimensions in each historical epoch, in each society, and is different for each person and depending on the circumstance in which it is subjected, it also molds and matures during each individual life period.

What is privacy for a teenager today certainly does not correspond with the meaning for an elderly person. This is not only due to technologies, but because the concept matures in each one and develops in different perspectives even within a single person.

That is, the idea of privacy also varies throughout a lifetime. Each human being can change the perception of what should be private according to personal development or even according to a certain circumstance in which is subjected.

Children's social relationships and adolescents pass through technology. Exchange of messages, exposure of sexuality, among others, are part of the experimentation of the discovery of being. The big dilemma today is that these trials take place online, under the wake of Big Brother who forgives nothing and that nothing forgets.

This work will not seek to understand or criticize the individual exposure and the limits that each one establishes for himself. The concern is not to respect these individually imposed limits through consent. Or, as in the case of children, not having the complete discernment to establish such barriers.

---

[213] MOORE, Adam D. **Privacy rights**: moral and legal foundations. Pennsylvania: The Pennsylvania State University Press, 2010, p. 11.

Floridi[214] addresses how information and communication technologies (ICT) cause changes in the sense of identity, how people relate to each other and how they interact with the world.

Technology, especially in recent years, has radically changed self-perception, which is meant by "human being" and "world"; what's real, what's interesting… In this sense, Floidi[215] classifies three previous revolutions until reaching the current, and fourth, based on human self-perception.

In a first rupture, the human being, from Copernicus, realized not to be the center of the Universe. The second rupture took place from Darwin, who claimed not to be the center of biology, nature. What's left would be the center of consciousness. The idea that at least the human being is the master of their own thoughts. Freud then caused this third rupture by stating that even this centrality is not true.

The fourth revolution, then proposed by the author, from Turing, would again be affecting the centrality of the human being. They would no longer be the center of the universe, of nature, nor of their thoughts, nor of their “agency”.

This is because the artifacts that were created by technology are not as intelligent as the human being and will probably never reach the Hollywood imagination. However, they perform certain actions better than people. And that would alter the self-perception of what it's like to be a human being. In one example, if the taxi driver is not the one who determines the best path between point A and point B, the question of "then who am I?" is born. What today then means being autonomous, free, or intelligent, whether computers determine the best route, what we should buy or what movie we would like to watch[216]?

Although there is a perception that a great change is happening in the way the world is experienced, there is still no clarity of how and the whys of this revolution for the population in general.

---

[214] FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014.
[215]FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014.
216 FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014.

Despite the concerns regarding the new scenario, which are justifiable, it is also possible to glimpse enthusiasm for the changes to come. It's a new world, which it calls the "inphosphere"[217], that is being created and that can gain positive contours, for which future generations will be grateful, depending on the decisions made today.

Leaving the generality of the influence of surveillance on people's lives, it is possible to enter the peculiarities of the child public and their hypervulnerability.

There is inequity in knowledge and power when we confront the data subjects and who collect it. When this asymmetry is substantial, as in the case of childhood, the level of protection needs to be different. Perhaps the term asymmetry (used in the Brazilian data protection law) should be set aside and absorbed the vulnerability that deals with the Consumer Protection Code, at least in relation to minors.

That's because it's not just a superficial issue that can lead to bad choices. It is a substantial issue that has often perpetual implications for children's lives that will be impacted by choices sometimes made in disfavor of their best interest.

To consent that the child is vulnerable to the data economy is to say that there is no full autonomy of the will in their choices, and that, even that of their parents, they should be interpreted from their best interests[218].

3.1.2 Why we must protect children's privacy

The idea of protecting privacy is not an end in itself, but a tool to achieve other important values for the construction of being. Privacy will be treated here as necessary to consolidate the autonomy, self-determination, and protection of the child (integrity). Each will be understood in a distinct topic.

---

217 FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014.

218 This approach will be further elucidated in the last chapter.

3.1.2.1 Autonomy

First, it is necessary to delimit that the autonomy intended for childhood is not to place it in the level of "autonomy of will" typically brought by the Civil Code. Autonomy, presented here, does not refer to the freedom of negotiation or the ability to consent to a contract, but rather in its practical and everyday sphere of human development.

Thus, autonomy is given by understanding the rules as a stage of people's moral development.

While studying moral development, Piaget was concerned about the cognitive processes underlying it and defined stages through interviews and observation of children in rules games[219].

> Piaget points out that generally the moral rules that the child learns to respect already reach it elaborated by adults, especially by parents, that is, they already arrive as truths. [...] In this way one can examine how the rule is practiced: whether it is something sacred (henomous) or something about which one can decide whether to obey (autonomous) (free translation)[220].

That is, autonomy would be a phase of mental development in which the child acquires awareness and mastery of the rules of "games", which would occur gradually until the age of ten.

> (a) in the first stage (0-2 years old), marked as motor stage, children do not make use of rules, there is simply a motor and individual manipulation of the balls, there is no social activity, exploited balls seem to serve more to a physical knowledge of the object; (b) in the second stage (2-5 years old) called by Piaget as egocentric, children receive from abroad coded rules and play imitating the example, but there is no interest in finding partners to play or win the game, because the rules are used individually, each child plays for himself, even when in a group; (c) in the third stage (7-8 years old) characterized by Piaget as the stage of cooperation, the importance of winning the game arises; therefore, there is a need for the systematization of the rules, although in the same match there are variations regarding the general rules of the game; (d) in the fourth stage (11-12 years old) the rules of the game are set and understood thoroughly by all players. Piaget characterizes this stage as the codification of the rules, because now the

---

[219] Piaget, Jean. **O juízo moral na criança** (E. Lenardon, Trad.). São Paulo, SP: Summus. 1994. (Original published in 1932)

[220] QUEIROZ, Sávio Silveira, RONCHI, Juliana Peterle e TOKUMARU, Rosana Suemi. Constituição das Regras e o Desenvolvimento Moral na Teoria de Piaget: Uma reflexão Kantiana. **Psicologia**: Reflexão e Crítica, 22(1), 69-75, 2009, p. 70.

rules are part of society[221].

These rules, as pointed out, would be placed primarily by parents. However, from the perspective of data collection, the rules that are imposed on children are not formulated by parents, but by the strength of the market that has the interest in forming consumers.

In this game, the child will never unravel the coding of the rules, as it was not made for it to win. In this game, of marked cards, the contents are delivered according to the analysis of previous behaviors that drive to what companies think should be targeted.

This means that even if searching for the same information, different people will have different results as a result of previous searches, or a profile created through other data control mechanisms.

The big problem, in this case, is the lack of intellectual freedom as the right of the individual to receive information from different points of view, without restrictions imposed by those who do not have the competence to educate (advertising, companies, commerce...)

Or, from Piaget's analysis, to reach autonomy through the moral development of the understanding of the rules. However, if even adults cannot fully understand the rules of algorithmic games, how to demand so much from a child?

The more personalized the searches, the less chance that child will have of knowing a counter position or an idea different from the one already provided.

The lack of intellectual freedom correlates to cast within pre-established profiles from the previous learning of the algorithm that could guide future decisions of children attached to the panopticon of hidden interest or to simply cyclical choices. To be exemplified: a child who researched on flat earth, from a certain moment, all other research would lead to this content, consisting of truth within its range of informational possibilities.

---

[221] QUEIROZ, Sávio Silveira, RONCHI, Juliana Peterle e TOKUMARU, Rosana Suemi. Constituição das Regras e o Desenvolvimento Moral na Teoria de Piaget: Uma reflexão Kantiana. **Psicologia**: Reflexão e Crítica, 22(1), 69-75, 2009, p. 70.

The threats are clear by making an analogy to the alleged fraud in the U.S. election in which Trump was elected.

The suspicions are that, through the collection of voter data, the exact niche of undecideds was found. From then on, advertising was directed, masked as news, highlighting the qualities about the candidate, and criticism against the opposing candidate. The most serious thing about this case is that much of the news was fake. Thus, there was a turn in voting intentions that led the candidate to victory. In other words, a public opinion was formed based on information not checked, from a very efficient algorithmic targeting, which reflected the very idea of democracy, as a choice, of the people from the country[222].

However, when the target audience is children, the lack of previous personal development makes it extremely vulnerable to this practice. Children certainly do not elect their presidents, but they elect, for themselves, behaviors, beliefs, and motivations that will accompany them for the rest of their lives. This construction of personality can be shaped in the infantile phase not only by the good intentions of parents, teachers, and family members in assisting in the development of the child, but also by an economic force that aims only at profit.

In this case, the monitoring of this data for advertising purposes, the object of this research, can be equally dangerous.

Thinking about advertising targeting sometimes is even very well-seen. It may seem that it is possible to have only the advertising that really matters, receive exclusive offers, etc. However, not only issues related to consumerism, but also what to consume, or why consuming a certain product or service can be developed to the detriment of the child's autonomy to be who he/she wants to be, and not who advertising, or the internet, wants him/her to be.

Thus, children and adolescents, people still in development, should have their privacy and data protected in a priority, because information and communication

---

[222] BENNETT, Collin. J. LYON, David. **Data-driven elections**: implications and challenges for democratic societies. Internet Policy Review, 8(4) 2019. Available at: <https://doi.org/10.14763/2019.4.1433> Accessed 25 Jul., 2022.

technologies (ICTs) are able to remodel their own “self”[223].

Another point is when this data becomes public due to lack of storage security, or deliberately, as we have seen in numerous cases in recent years and will be deepened in item 4.8.

The idea of having exposed – and recorded forever, their mistakes, successes, or searches, compromises the autonomy of that individual. It will forever be, for others, and perhaps even for themselves, the description of what has been exposed.

The exercise of judgment, or autonomous thinking, according to Westin[224]

> requires time for sheltered experimentation and testing of ideas, for preparation and practice in thought and conduct, without fear of ridicule or penalty, and for the opportunity to alter opinions before making them public... Without such time for incubation and growth, through privacy, many ideas and positions would be launched into the world with dangerous prematurity.

That is, it is from experimentation, made in privacy and without the eyes of surveillance, that autonomous thinking develops.

Still, the very fact of feeling that it is being watched makes the experience completely different, as seen in item "3.1.1 the effects of surveillance". In this case, it seeks not only what is in its conscious and moral, but also the expectation of others about that behavior. And so, once again, autonomy is tolled.

3.1.2.2 Self-determination

In addition to involving what is thought, as autonomy and intellectual freedom, privacy is also a tool of self-determination. That is, to act according to your free thinking. Closely linked, then, to the previous topic. However, conditioned actions are more related. In this context, privacy is not only a right of seclusion, but mainly of freedom. Freedom to think and behave freely from the shacks of continuous vigilance. Just as seen in the vertical dimension of the basic typology.

---

[223] FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014, p. 122.
[224] WESTIN Alan F., **Privacy and Freedom**. New York: Ig publishing, 1967, p. 33.

Sometimes the two terms (autonomy and self-determination) are used as synonyms. This is not the case with the analysis, because it is understood that the child is especially influenced to act, even if there is no previous reflection on such behavior. Self-determination is the ability to decide free of coercion.

Privacy assumes "a relational character, which must determine the level of the relationship of one's personality with other people and with the outside world – by which a person determines their insertion and exposure" (free translation)[225], that strengthens the individual in his "free development of personality, without the pressure of mechanisms of social control"(free translation)[226].

The general privacy interest that is being threatened by the children's data collection involves the individual's right to control information about his or her person.

From the perspective of data protection, informational self-determination is related to the ability to determine and control the use of data. In this sense, represented by the parents.

The mere fact that a complete personal profile of a single individual is compiled is a threat to privacy. The maintenance of this information over time and the various uses it may have, outside the initially directed purpose, puts the situation out of control.

Although certain information seems to be harmless when provided, the future consequences, including for adulthood, of this child are certainly outside the level of control or cognition possible about it.

Giving total self-determination to children is incompatible with their condition of being developing and devoid of civil responsibilities without representation.

In this sense, some norms, such as COPPA, and LGPD, have placed parents as central to generating consent for data collection, and thus make it

---

[225] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 131-132.
[226] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 132.

absolutely lawful.

Parents, however, also lack clarification and are often unaware of the dangers to which they are exposing their children. In this sense, to think that the decisions made by them will remain perpetually, even in the adult life of children, does not seem to be coherent. In the last chapter of the thesis, the need for reassessment of the theory of consent, adequate representation and the possibility of opt-out when adulthood is reached, of any collection related to children will be addressed.

Finally, if one of the aspects of privacy is the individual control over information and self-determination of how to manage it, this is also lost due to the lack of regularization or the lack of effectiveness of the regularization of data collection and use. Failure to consent and other transnational principles of data protection is a way to restrict the informative self-determination of the individual (or in this case, of his/her parents) about his/her data.

3.1.2.3 Protection/Security

Although security is not the object of this work from the perspective of state protection, it connects to the subject when the data that was collected for commercial use is leaked.

That is, data that was originally collected for commercial use and that end up being used by a third party, without the consent of those who provided or who stored the information for illicit purposes.

An example of this situation would be photos of children collected in a medical context, leaked from databases, and forwarded to child pornography websites.

Or geolocation data, which should, at first, keep the child on the watch of parents or other authority, which end up being used for screening, kidnapping, or other related crimes.

Regardless of whether this dissertation does not address the issue of child safety or state protection, it is indisputable that the last degree of threat suffered by a

child to having his information exposed is to his physical integrity.

In this sense, the data breach topic will be addressed in item 4.8.

3.2 Regulation of children's advertising in Brazil

The collection and use of data may have several purposes, as seen. However, this work was restricted to its use for commercial purposes. That is, when a company collects the data, in the case of children, so that this generates economic benefit as a result in sales.

The focus of the use of data in this limitation is for advertising. That is, data is collected to generate a user profile that will serve as the basis for advertising to be increasingly specific and effective, achieving its goal of persuasion to the sale of the product, service, or even the brand.

In the case of children, as will be seen in the following chapters, there are specific restrictions for the collection and treatment of data, which are almost always conditional on the consent of parents or guardians.

Other restrictions on children's advertising go beyond data collection, but which are equally of interest to work because they are intertwined with the general objective: to understand and/or improve the regulation of the media in the advertising context, for children.

On this theme it is necessary to differentiate the theoretical debates and practices, which differ.

The thesis in force and supported especially by the Alana Institute through the program "Child and Consumption", with the interpretation of CONANDA (Conselho Nacional dos Direitos da Criança e do Adolescente) resolution 163/2014, is that all children's advertising is prohibited in Brazil[227].

---

[227] INSTITUTO ALANA. Criança e consumo. **Publicidade infantil é ilegal**: entenda o impacto da Resolução 163/2014 do Conanda. Available at: <https://criancaeconsumo.org.br/wp-

The interpretation is based on Article 36 of the Consumer Protection Code[228], in which the principle of mandatory identification of the advertising message is provided: “advertising must be shown in such a way that the consumer, easily and immediately, identifies it as such” (free translation).

In other words, advertising should be recognized as advertising by the target audience to which it is intended in order to protect the consumer and make him aware that he is the recipient of a sponsored message that has commercial purposes, differing, for example, from journalistic content. “This principle serves on the one hand, to prohibit so-called subliminal advertising, which in the CDC system would be considered a practice of civil and even criminal unlawful act” (free translation)[229].

Besides,

> Advertising is only lawful when the consumer can identify it. But that is not enough: identification must be immediate (at the time of exposure) and easy (without effort or technical training). Advertising that does not want to assume its quality is an activity that, in one way or another, tries to deceive the consumer. And deception, even the innocent, is repudiated by the Consumer Protection Code[230].

The article seals the practice of “merchandising”, known in Brazil as commercial insertion during content without the clear interruption of this. It is the products placed in the middle of a television program, or even the allusion to a particular brand during a journalistic news, for example.

Following the law, Article 37 prohibits all abusive advertising, and characterizes as such, among other circumstances, that which is used by the child's deficiency of judgment and experience.

In this argument of abuse from childhood immaturity, or hypervulnerability,

---

content/uploads/2014/02/Publicidade-Infantil-%C3%A9-ilegal.pdf> Accessed 05 Sep., 2022.

[228] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de defesa do consumidor**. Legislação Federal.

[229] LIMA MARQUES, Claudia. **Comentários ao Código de Defesa do Consumidor**, 2ª edição, Editora Revista dos Tribunais, 2006, p. 529.

[230] HERMAN BENJAMIN, Antonio. **Código Brasileiro de Defesa do Consumidor**, 6ª edição, Editora Forense Universitária, 1999, p. 277-278.

is that the notion that rational decision-making process does not apply to children is born, being “too young to understand the necessarily partial nature of the advertising message” (free translation), which would generate, as a consequence, the thesis that “any advertising directed at children under a certain age does not cease to have enormous abusive potential”[231].

It, therefore, interprets the Alana Institute which

> In fact, for those same reasons, one can go further, say that any advertising directed at children – considered persons under the age of 12 – is intrinsically abusive, since, if they do not understand the partial nature of the advertising message, they are unable to understand it as such, and therefore they will always be having their disability of judgment and experience exploited by advertising (free translation)[232].

The National Council of Advertising Self-Regulation (CONAR), through the Brazilian Code of Advertising Self-Regulation, prepared by members of the advertising class itself with the objective of ensuring an ethical activity, honest and in tune with the values of Brazilian society, does not corroborate the thesis of prohibition of children's advertising. However, it recommends in section 11[233] that “the efforts of parents, educators, authorities and the community should find in advertising an adjunct factor in the training of responsible citizens and conscious consumers”, so being, “no advertisement will address imperative consumer appeal directly to the child” (free translation).

That is, advertising directed at the child could happen, but being restricted to some rules: the first, found in the caput, that the ad cannot have imperative appeal. That is, words like "buy", "use", "ask" etc.

Ads should have positive social values, as among others, good manners, “friendship, urbanity, honesty, justice, generosity and respect for people, animals and

---

[231] HERMAN BENJAMIN, Antonio. **Código Brasileiro de Defesa do Consumidor,** 6ª edição, Editora Forense Universitária, 1999, pp. 299-300.

[232] INSTITUTO ALANA. Criança e Consumo. **Normas em vigor**. Lei nº: 8.078/1990 – Código de Defesa do Consumidor (CDC) comentado. Available at: <https://criancaeconsumo.org.br/normas-em-vigor/codigo-de-defesa-do-consumidor-cdc-comentado/> Accessed 18 Jul., 2022.

[233] CONSELHO NACIONAL DE AUTO-REGULAMENTAÇÃO PUBLICITÁRIA – CONAR. **Código Brasileiro de Auto-regulamentação publicitária**. Available at: <http://www.conar.org.br/codigo/codigo.php> Accessed 18 Jul., 2022.

the environment"[234].

In addition, they should refrain from discriminatory ideas; children's association with illegal, dangerous, or resonant situations; impose the notion that the consumption of the product provides superiority or, in its absence, inferiority; cause situations of embarrassment to parents or guardians; use of children as models of recommendation or suggestion of use; use journalistic format that confuses advertising[235]...

Therefore, advertising targeted at children should

> (a) contribute to the positive development of parent-child relationships (...);
>
> (b) respect the dignity, ingenuity, credulity, inexperience and feeling of loyalty of the target audience;
>
> (c) pay special attention to the psychological characteristics of the target audience, presumed its lower capacity for discernment;
>
> (d) such care that avoids possible psychological distortions in advertising models and target audiences;
>
> (e) refrain from stimulating socially reputable behaviour (free translation)[236].

The code also condemns, in accordance with the Consumer Protection Code, merchandising practices or indirect advertising, which use children or elements of the children's universe that have the child as a target audience, by any communication vehicle used[237].

That is, the interpretation of the Consumer Protection Code in relation to child advertising is of total restriction by the Alana Institute, and partial restriction by the Advertising Self-Regulation Council (CONAR).

The National Council for the Rights of Children and Adolescents (CONANDA), in its Resolution 163/2014[238], dealt with the abuse of the advertising

---

[234] Art. 37, 1, a.
[235] Art. 37, 1, b-i.
[236] Art 37, 2.
[237] Art. 37, 4-5.
[238] BRASIL. CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE –

and marketing communication targeting children and adolescents[239].

Article 2 of that resolution considers abusive

> (...) the practice of directing advertising and marketing communication to the child, with the intention of persuading them to consume any product or service and using, among others, the following aspects:
>
> I - children's language, special effects, and excess of colors;
>
> II - soundtracks of children's songs or sung by children's voices;
>
> III - child representation;
>
> IV - people or celebrities with appeal to children;
>
> V - characters or children's entertainers;
>
> VI - cartoon or animation;
>
> VII - dolls or the like;
>
> VIII - promotion with distribution of prizes or collectible gifts or with appeals to children; and
>
> IX - promotion with competitions or games with appeal to children.

It is also important to highlight the definition of marketing communication brought by Resolution 163/14, any commercial communication activity, including advertising, for the dissemination of products, services, brands and companies, carried out through any media, covering, among other tools, print ads, television commercials, radio spots, banners and web pages, packaging, promotions, merchandising, actions in shows and presentations and at points of sale.

Herman Benjamin, one of the CDC co-authors, stresses that the legal definition of advertising, strongly inspired by Belgian consumer law, considers all "information or communication disseminated for the direct or indirect purpose of promoting, with consumers, the purchase of a product or the use of a service,

---

CONANDA. **Resolução 163/2014**. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Available at: <https://crianca.mppr.mp.br/pagina-1635.html> Accessed 18 Jul., 2022.

[239] There is discussion against the binding force of the resolution, since CONANDA does not have the power to apply any kind of penalty, which would make the resolution only a guideline without normative force.

whatever the place or means of communication used" (free translation)[240].

These definitions put an end to the endless discussions on the differentiation of the terms "publicidade" and "propaganda" in Portuguese, or the scope of the term beyond the spaces dedicated in television, radio, tv, magazines and other traditional media. This is therefore, the Brazilian legislation does not differentiate the terms and treats them indiscriminately in its texts, making no sense to have any kind of classification – not even by the didactic issue – given the lack of practical relevance for this.

Thus, when talking about "marketing communication" there is broad talk of any type of activity with commercial purposes, which includes, but is not restricted, to advertising. It therefore also involves packaging strategies, marketing, point of sale, etc.

It was only in 2016 that the Superior Tribunal of Justice stood categorically on the matter, through the trial of Special Appeal No. 1558086, declaring that advertising to children in Brazil is prohibited.

The case dealt with the campaign of the Bauducco brand[241], in which it conditioned, in combined sale, a wristwatch witan h image of children's characters to food products, then declared as abusive advertising.

Minister Humberto Martins, rapporteur of the appeal, understood to bit e a case of gift simulation, inducing the consumer to behave unwantedly, when in reality he would be conditioning one purchase to another.

This is not, however, the historical factor given to the decision, since such abuse (of the combined sale) is expressly provided for in the Consumer Protection Code, article 39, I in which it prohibits the practice.

---

[240] BENJAMIN, Antônio Herman V; MARQUES, Claudia Lima Marques; MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019. E-book.

[241] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1558086**. Relator: Ministro Humberto Martins, j. 10.03.2016

The great turn point is in the part where it is considered abusive the advertising of food, as well as medicines, directed at children. According to the same,

> the child does not have the legal consent capable of completing the legal business, but has the power of convincing, from the cry to other more subtle acts, in supermarket, outside the supermarket, the bullying of other colleagues who have Shrek's watch and this poor child that parents try at all costs to educate in their own way, has not (free translation)[242].

Thus, there was the recognition that food advertising is abusive by the simple fact of addressing the child; in addition to the clear content of combined sale that the case presented.

These positions are full of gaps that reflect a reality that is detonating from the theory presented. To advance the discussion on the theme in the direction of uniting theory and practice it is necessary to understand the critical points in question, as will be seen below.

3.2.1 Criticisms and limitations on current positioning

The first critical point to the current position is the conceptual limitation of the term advertising within the Brazilian legal system.

As already mentioned, the legislation itself makes confusion between the terminologies "publicidade" and "propaganda", treating them as synonymous. Furthermore, new ways of communicating the ideas, products and services of a brand with its consumers are all the time updating the possibilities of what is considered as advertising.

For this reason, CONAR's resolution included, together with advertising, a "marketing communication"[243], as a way to expand the scope, as seen in the previous topic.

---

[242] Audio available at: <http://www.migalhas.com.br/arquivos/2016/3/art20160310-07.mp3> Accessed 05 Sep., 2022.

[243] BRASIL. CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE – CONANDA. **Resolução 163/2014**. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente. Available at: <https://crianca.mppr.mp.br/pagina-1635.html> Accessed 18 Jul., 2022.

It is not possible only to totally prohibit advertising and not to consider that the characters, colors, the position of a particular product in the store, the packaging, the opinions of influencers, for example, are also part of this universe.

To completely ban advertising would prohibit the use of characters in product packaging, or even colors that could refer to a "marketing communication" aimed at children.

In this way, there is also the difficulty of quantitative restriction beyond traditional media. It is no longer possible to imagine a limitation in the percentage of time or quantity when the child is exposed to different forms of advertising, often veiled, and in different media. The fluidity with which it migrates from content to content, from one social network to another or even within it, makes any kind of control in this sense impossible[244].

In addition, there are economic limitations that involve advertising as the main sponsor of the media. So that traditional media such as television, radio, magazine, newspaper, to gaming apps or websites, have as the main income for the content that is published in the marketing of advertising. Monetization can be performed in two ways: the sale of advertising space with prior analysis of the consumer profile, territorial coverage, among others; or, also, with the sale of the database with information from consumers for another purpose.

Anyway, it is advertising that keeps viable the production of programs, applications, games, among other media. Banning advertising altogether would also remove children's access to such content.

Finally, the limitations still go through the family's adherence, since, ultimately, the use of children depends on the consent of the parents, as will be seen in the next chapters and also explored in the latter.

And it's the parents or guardians who often circumvent age restrictions so that their children have access to certain content, game or app. They are the ones

---

[244] As clarified in the previous topic, the ideas of restriction are and headed by the project "child and consumption" of the Alana Institute, from the interpretation d and that all advertising directed to the child is prohibited in Brazil.

who filter consumption within their homes in a decision swelled by subjective criteria that go far beyond advertising.

3.3 The child as a product

As seen, if everyone is vulnerable to media strategies[245], children can be classified as hypervulnerable due to the difficulty of identifying the advertising message on the Internet[246] given the confusion between reality and fantasy, media seduction, as well as the difficulty of reaching "free consent", as a principle of the right to data protection (how it will be explored in the next chapter).

The Regional Center for The Development of the Information Society (Cetic.br), as part of an international study, explored the perceptions of children and adolescents about their rights in relation to digital media. It is especially noteworthy that internet access it seems to them ensure their rights to freedom of expression, access to information, privacy, education, and recreational activities[247].

These children have a positive view of the Internet and are experiencing the main characteristics of identity building their ability to interact between peers and with other reference people, as well as their achievement of autonomy, in an online and offline environment that interact fluidly.

Digital natives start using the internet earlier and earlier and feel comfortable and familiar with the features. Thus, they often do not realize the risk or have a sense of the longevity of the data given. There is no assumption of prior mistrust when this technology is incorporated into everyday life in such an organic way. Belief in anonymity also reduces family protection from the risk of exposure. Families who do not understand the digital traces and risks related to these can be a

---

[245] From the idea that every consumer is vulnerable, from the Consumer Protection Code, art 4º, in. I.
[246] As provided in the caput of Art. 36 of the Consumer Protection Code: "advertising must be identified in such a way that the consumer, easily and immediately identifies it as such".
[247] COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. (2020). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: **TIC Kids Online Brasil 2019**. São Paulo: CGI.br. Available at: <https://cetic.br/media/docs/publicacoes/2/20201123093344/tic_kids_online_2019_livro_eletronico.pdf > Accessed 27 May, 2019.

mitigating factor in the protection of child privacy[248].

However, understanding what digital traces children are creating for their future is essential to the debate of the necessary preventive and repressive promotion of the state in their defense. Since there is no rubber in the world that erases 100% what is on the Internet.

The fact is that children are exposed to informational exchanges with potential data storage. Be it from "smart" toys, personal assistants, smartphones, computers, *smart* TVs, surveillance cameras among many other possibilities.

All data collected from these traces creates a user profile and integrates the "online reputation". This reputation, which for digital natives, has as much or greater relevance than the offline.

Consumer characterization in traditional media – radio, television, and print media – was traced by a likely audience diagnosis. It was known, for example, that in the morning hours more children and housewives watched TV, thus, programming and, consequently, advertising, were aimed at this public. By night, during the hours of the news, the advertising became more adult and masculine.

They are still very valuable data on the consumer, but quite generic compared to the possibilities of identification through digital media.

This is therefore, through the registrations in the applications and the use of cookies and other tools to trace not only the data that registers, but the profile of pages visited, searches, etc., it is accurately identified not only the age group and gender of the consumer, but strictly individualized data, as seen.

---

[248] Research reveals that 70% of parents or guardians believed that children and adolescents made safe use of the Internet. On the other hand, 50% of children and adolescents who use the network reported that their parents or guardians know more or less or nothing about their Internet activities. In addition, 70% of Internet users aged 11 to 17 had the perception that they know many things about using the network and 76% that they know more than their parents. PCOMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. Survey on internet use by children in Brazil: ICT kids online Brazil 2017 [livro eletrônico] / Núcleo de Informação e Coordenação do Ponto BR, [editor]. -- São Paulo: **Comitê Gestor da Internet no Brasil,** 2018. Available at: <https://cetic.br/media/docs/publicacoes/2/tic_kids_online_2017_livro_eletronico.pdf> Accessed 05 Apr., 2019, p. 122.

It is common check the requests for "like", "comment", "follow", "subscribe", "like it", "I want to know your opinion". Consumer participation is requested as a genuine interest in knowing who is on the other side of the "screen", as a very personal relationship of friendship and exchange. When, in fact, what is intended is that the user's support reverts to a positive "adhering" data to the publication, and, with this, increases the profit of those who disclose it.

Theoretically, free content is actually monetized through personal data. That is, the consumer also becomes a product in the relationship with the brand, as he feeds back that relationship by being constantly watched.

This sub-chapter will move on to the debate of the child as an advertising product (behavioral targeting), from the moment it ceases to be interesting only as being passive of the media relationship and becomes, actively, a builder of valuable information that will be directed to the construction of systematized profiles.

There are two ways to collect personal information from children, especially in the virtual environment. The first method is the asset, in which the child is asked directly about some data[249]. The second method, called passive collection, is performed without the child's knowledge or consent. Passive data collection includes clickstream data, IP addresses, cookies, and Web bugs[250].

The active method needs a child's action in deliberately providing whoever collects the requested information. According to the "Privacy Online: a report to Congress"[251], common examples are child name, email address, postal address, telephone number, age or date of birth, and gender. Some even ask information about where to attend children school, what sports they play, whether they have any siblings, what they have named their pets, and even whether they have time after school alone without parental supervision.

---

[249] Federal Trade Commission, **Privacy Online**: A Report to Congress. Available at: <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (June 1998). Accessed 05 May, 2022.

[250]HERTZEL, Dorothy A. **Don't Talk to Strangers**: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online, 52 FED. COMM. L.J. 429, 431 (2000).

[251] Federal Trade Commission, **Privacy Online**: A Report to Congress. Available at: <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (June 1998). Accessed 05 May, 2022.

The forms of questioning are varied and may typically be registration forms, order forms, surveys, contests, and games to gather this information[252]. According to the FTC[253], some Web sites use imaginary characters to request personal information. Other sites ask

> children [to] sign a 'guest book,' solicit information to create home pages for children, invite children to participate in chat and electronic pen pal programs, require children to register with the site for updates and information, and offer prizes and other incentives for completing surveys and polls.

Yet, children commonly reveal personal information while participating in chat rooms or posting messages on electronic bulletin boards.

The child is already quite vulnerable to giving given, knowing that is doing it, because, due to his immaturity, it does not yet understand the possible consequences of choices. Consequences that are difficult, even, for adults to understand in their greatness.

However, the second method is even more worrying and escapes the control, including of parents, in the education of their children. If, in the first situation, it is still possible to guide the children not to reveal their information, as well as to "not talk to strangers", when talking about passive data collection, the child's behavior will have little influence on the data to be collected or not.

The second method of collecting information, passive data collection, is less obvious because it is collected surreptitiously. Each time a person visits a particular site, an electronic vestige is left whereby the individual unknowingly provides valuable information to the Web site operator.

The type of information revealed includes the user's Internet service provider, type of computer and software, the site from which she linked, the files

---

[252] FEDERAL TRADE COMMISSION **Privacy Online**: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000). Available at: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> Accessed 4 May, 2022.

[253] FEDERAL TRADE COMMISSION. **Privacy Online**: A Report to Congress. Available at: <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (June 1998). Accessed 4 May, 2022.

accessed, and the amount of time she spent on each page. Websites gain this type of information by setting cookies[254], which effectively gather information without the user's knowledge, and are useful to personalize the browsing experience. Once a cookie is set, the user's computer is assigned a unique identifier so that the user can be recognized in future visits to the site. "Cookies alone cannot divulge your name or address, but they can reveal how long you stay at a page, which products you like, and which sites you visit"[255].

The information collected actively and passively, are so common that almost all sites analyzed in the may 2000 Report of the FTC obtain an e-mail address or some other type of personally identifiable information. In additional, the FTC found that 86% of these Web sites fail to disclose their information practices. And more worryingly, the report pointed out that websites were collecting personally identifiable information also commonly collect several other types of information that enable them to form a detailed child profile[256].

Although some of this information individually does not identify the user, combined with many other collections provides an individualized profile that can be used by advertising to target their demands to a strategically delimited audience.

The use of cookies, in turn, is not completely bad nor can it be simply banned. Tracking online navigational patterns, commonly by employing cookies, is useful for the website to make improvements to its own site and to personalize the user's online experience.

It is through it that, once a product has been placed in the "shopping cart", when searching for other products in the same e-commerce, the cart will continue

---

[254] Cookie is information saved by the web browser when someone visit a website, so it can recognize the device in the future and keep tracking over time. FEDERAL TRADE COMMISSION. **Internet Cookies**. Available at: <https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies> Accessed 04 May, 2022.

[255] MATLICK, Justin. The Future of the Net: Don't Restrain Trade in Information, **WALL ST. J.,** Dec. 2, 1998.

[256] FEDERAL TRADE COMMISSION. **Privacy Online**: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000), Available at: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> Accessed 04 May, 2022.

filled with the choices previously made. Usernames, preferences and other data are also saved through this system which certainly facilitates navigation.

The information allows the website to monitor and understand what attracts children to the site and then tailor the site's content and services based on the children's identified interests[257].

However, the most profitable way to use personal information is when it is collected or sold to marketing services for the sole purpose of exploiting the sale of products or services, from the targeted profile, as follows:

3.3.1 Targeted ads

Advertising has always been looking to identify your target audience so that your efforts are better contemplated. Knowing who are talking to, it is possible to save resources from unsuccessful attempts to communicate and direct the content knowing, in advance, what is expected and what most easily convinces that person to brand loyalty or the purchase of a particular product or service.

With technological advances it became possible to trace this profile and in an increasingly individualized way.

It was known, for example, that at a certain time there is a greater propensity for children to be watching TV. However, when placing an ad on a television channel at that time, there was a huge chance that children were not actually watching, as well as reaching an audience other than the intended one.

Today, with the use of cookies and other ways to trace enhanced profiles of users, it is possible to know exactly who they are communicating with, and thus outline a more effective and inexpensive strategy to have the desired effect: consumption.

---

[257] GINDIN, Susan E., Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 **SAN DIEGO L. REV.** 1153, 1170 (1997).

Direct marketers capture children's attention online through one-to-one marketing that effectively bypasses parents and teachers to directly reach children. The tracking technology enables companies to follow every interaction between a child and an advertisement[258]. “The ultimate goal is to create personalized interactive ads designed to 'micro-target' the individual child"[259].

Trading this data is highly profitable for those who make both public and private data lists and sell to third parties. And these lists generate other lists that feedback to increasingly specified profile IDs for different interests[260].

Marketing strategies are based on the influence children have on their parents' spending. In 1995, in a pre-internet and pre-targeted ads era, children, together with teenagers, influenced $160 billion of their parent’s annual spending[261]. The numbers, of course, will never be able to specify how much of the children's consumption is decided voluntarily by their parents and how much they are influenced. However, given the growing market strategies for reaching this audience, there is no denying that it is a growing and profitable market. An opportunity also to retain, from an early age, a consumer to a brand.

The value of children's personal information is undeniable, but the collection and use of the information create great potential for misuse and threatened privacy of children.

3.3.2 Native advertising or merchandising

Classic advertising, which appears for example as a "banner" or interrupting a video, can be abusive when using consumer data without consent, for

---

[258] CENTER FOR MEDIA EDUCATION (CME), **Web of Deception**: Threats to Children From Online Marketing (1996). Available at: <http://www.cme.org/children/marketing/deception.pdf> Accessed 04 May., 2022.

[259] CENTER FOR MEDIA EDUCATION (CME), **Web of Deception**: Threats to Children From Online Marketing (1996). Available at: <http://www.cme.org/children/marketing/deception.pdf> Accessed 04 May., 2022.

[260] SAFIER, Seth, Between Big Brother and the Bottom Line: Privacy in Cyberspace, 5 **VA. J.L. & TECH.** 6, 29 (2000).

[261] SAFIER, Seth, Between Big Brother and the Bottom Line: Privacy in Cyberspace, 5 **VA. J.L. & TECH.** 6, 29 (2000).

example. But in general, it is lawful advertising, as discussed in its own topic.

Another type of advertising, however, has been gaining strength, especially among children. Called “native advertising” or “sponsored content”, which are articles paid for or written by brands as a powerful advertising tool that has left the limits of traditional media and major publishers to invade social networks as well.

Appearing an unpretentious testimony to a "great" new product, digital influencers are used as marketing tools to attract their legions of followers to consume the same products.

If there was a clear mention that this is an advertising message, its lawfulness could still be discussed, due to the target audience it reaches, as seen in the previous item.

However, if there is no such mention, there is no doubt that it is a type of "merchandising" or "indirect advertising", in which the content and the advertisement mix without own lines that define them as such.

Thus, especially when for children, the lack of definition of advertising content makes it abusive, and therefore unlawful.

However, these forms are widely used in Brazil and have often seen cases of appeals from the Alana Institute to the Brazilian judiciary.

In 2021, 9 companies were targeted for referral of representation by the institute to the Public Prosecutor's Office of the State of Bahia for the practice of abusive advertising, consistent in the development of marketing communication strategies directed directly to children, which are: Sunny Brinquedos, Hasbro, Ri Happy, Xplast, DTC Trading, Fun, Criamigos, Compactor e Stabilo.

> The actions consisted of the use of children's channels on the YouTube platform, for the dissemination of products, promotions, and services, in the case of toys and school supplies.
>
> In general, companies send their products for children to advertise on their channels. As they are children speaking directly to other children, the identification process fulfills even more effectively the goal of companies to develop consumerist desires in small, in a clearly abusive way.

> Thus, it was considered that companies exercised abusive and illegal practice, because they take advantage of the vulnerability of children YouTubers and children spectators to leverage sales of their products[262] (free translation).

As there is still no progress in the process, it is not possible to discuss the outcome of it. However, in 2016, similar representation was forwarded, containing 15 companies denounced by the same practice: Bic Graphic Brasil Ltda, Biotropic Cosmética Licensing, C&A Modas Ltda., Cartoon Network, Foroni Indústria Gráfica Ltda., Edutenimento Entretenimentos do Brasil Ltda. (Kidzania), Long Jump – Representação de Brinquedos e Serviços Ltda., Mattel do Brasil Ltda.,Arcos Dourados de Alimentos Ltda. (McDonald's), Pampili Produtos Para Meninas Ltda., Lojas Puket Ltda., Ri Happy Brinquedos S.A., Sistema Brasileiro de Televisão – SBT, Sestini Mercantil Ltda.e Tilibra Produtos de Papelaria Ltda.

In this case, the Federal Prosecutor's Office of Rio de Janeiro opted for the archiving of the investigation on the grounds that it would not have the task to conduct the action. This is because the companies are located in the State of São Paulo, and it is then up to the prosecutor of The Children and Youth of that State to investigate the facts and adopt protective measures to safeguard the minors in question[263].

However, as result of this complaint, in 2017 the Public Prosecutor's Office of the State of São Paulo filed a Public Civil Action against Google[264], company owner of YouTube, asking for the removal of videos published in channels of child influencers, due to veiled child advertising of the brand Mattel.

In all, 105 videos from seven channels were cited. In addition to the removal of the videos, the lawsuit also called for Google to adopt surveillance and usage measures to prevent the use of YouTube for children's advertising.

---

[262] ALANA. Criança e Consumo. **9 empresas**: Publicidade infantil em canais de YouTubers Mirins (agosto/2021) Available at: <https://criancaeconsumo.org.br/acoes/9-empresas-publicidade-infantil-em-canais-de-YouTubers-mirins-agosto-2021/> Accessed 18 Jul., 2022.

[263] ALANA. Criança e Consumo. **15 empresas - Canais de YouTubers Mirins:** Publicidade na Internet (março/2016) Available at: < https://criancaeconsumo.org.br/acoes/YouTubers-mirins/> Accessed 18 Jul., 2022.

[264] Ação Civil Pública n. 1132354-36.2018.8.26.0100 (MP-SP x Google Brasil Internet Ltda)

The Public Civil Action was archived after Google and CONAR signed a Term of Agreement, pledging to develop a Manual of Good Practices in children's advertising in the digital environment[265].

The document, extremely succinct, perhaps unsatisfactory, makes no reference to the ban on veiled (native or sponsored) advertising and is restricted to dealing generically with the matter. As in item 5, where it highlights that

> The advertiser, the agency and any third parties hired by them, including influencers, shall seek, know and comply with the general rules and segments of the products disclosed, in particular the Statute of the Child and Adolescent, Consumer Protection Code and the Brazilian Code of Advertising Self-Regulation[266] (free translation).

As if knowing and complying with the rules of Brazilian legal order was no longer an obligation of all.

The document was criticized by the Alana Institute, since the debate of the action would take place, exactly, from the argument of the prohibition of advertising, which was not even mentioned in the agreement. Therefore, contrary to the cause of the request in the action, it could not close the dispute[267].

On the same object, there was also a Public Civil Action against Mattel[268]. In this, the company was ordered to pay compensation in the amount of R$ 200,000.00 for collective moral damages, in offense to the Consumer Protection Code and the resolution of CONANDA, since it employed child celebrity (prohibited by resolution), abused the deficiency of judgment of the child and did not make it clear to be advertising content.

The amount of compensation, provably, is lower than the costs that the company had with the marketing strategy or with its earnings.

Thus, even though this chapter exposed the relation to children's

---

[265] GOOGLE, CONAR. **Guia de boas práticas para a publicidade online voltada ao público infantil.** Available at: <http://www.conar.org.br/pdf/guia-infantil-conar.pdf> Accessed 08 Aug., 2022.
[266] GOOGLE, CONAR. **Guia de boas práticas para a publicidade online voltada ao público infantil.** Available at: <http://www.conar.org.br/pdf/guia-infantil-conar.pdf> Accessed 08 Aug., 2022.
[267] CRIANÇA E CONSUMO. **Mattel**: você YouTuber escola Monster High (fevereiro/2017). Available at: <https://criancaeconsumo.org.br/acoes/mattel-do-brasil-ltda-voce-YouTuber-escola-monster-high-fevereiro2017/> Accessed 08 Aug., 2022.
[268] Ação Civil Pública n. 1054077-72.2019.8.26.0002 (MP-SP x Mattel do Brasil Ltda)

vulnerability to the media, the effects of surveillance and the need to protect their autonomy, self-determination and security, there is still an intense debate in Brazil about the limits of the regulation of child advertising, with divergent positions on its scope.

In practice, what is seen is little effectiveness in the prohibition, although clearly there is an offense to federal law. The self-regulation, brought by CONAR, in this sense, serves as a shield of the industry to maintain the current market status little regulated, or little punished by the infractions.

Companies based outside Brazil, as highlighted in the last item, Google, maintain practices incompatible with the national legal system and rely on their own regulations to determine the limits of action.

For this reason, the next chapter will move forward on the principles of data protection, which appear on a transnational form, to ensure that the standards of each state, or companies, are compatible with the minimum expected protection.

CHAPTER 4
TRANSNATIONAL PRINCIPLES OF DATA PROTECTION

With the growing technology and massive use of the internet supported by the ability to electronically store information, privacy has gained new meanings, as seen.

Similarly, data privacy regulation is a global trend with significant changes in the legal systems of several countries, whose focus is to draw clear guidelines on the privacy and security of this information.

At least one hundred and forty-three countries and territories worldwide have adopted comprehensive data protection and or privacy laws; in addition to many others who have pending draft or law initiatives[269].

Despite differences in language, legal traditions and cultural and social values, there has been a broad measure of agreement on the basic content and core rules that should be embodied in data protection legislation[270].

These data protection laws and legal instruments contain an explicit set of data protection principles, which emerged especially from the 1980s[271]. The emergence of the global market has led to an increase in the exchange of information across national borders, resulting in data protection becoming an international issue.

The OECD (The Organization for Economic Co-operation and Development) elaborated in 1980 the Guidelines on the Protection of Privacy and

---

[269] IAPP. **Global Privacy Law and DPA Directory**. Available at: <https://iapp.org/resources/global-privacy-directory/> Accessed 01 Mar., 2022.

[270] BENNETT, Colin. **Regulating privacy**: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, p. 95.

[271] Refer as "fair information practices". FLAHERTY, David H. **Protecting Privacy in Surveillance Societies**: The Federal Republic of Germany, Sweden, France, Canada, and the United States. The University of North Carolina Press, 1992, p. 372-403.

Transborder Flows of Personal Data[272], based on the “Fair Information Privacy Principles”, idealized by the U.S. Department of Health, Education and Welfare (HEW), as a way to enhance the use of information technology and ensure privacy.

Although not binding between the member countries of the European Union, the document has become a reference for national law[273].

Soon after, the Council of Europe dealt with the matter at the Convention for the Protection of Individuals with Respect to the Automated Processing of Personal Data (108/1981), known as the Strasbourg Convention or Convention 108.

International organizations such as the OECD, the European Council and the European Economic Community (now the European Union) (EU) realized that if multinational corporations needed to comply with different data protection standards in each country in which they process or store data, would become overly burdensome. If it were not the case to comply with each country, the creation of data havens could be fostered (countries where there are no data protection regulations) that could nullify other countries' efforts to protect the freedoms of their citizens[274].

Countries, including from outside Europe, have ratified the Convention, applying their internal legislation or legislating for the first time on the subject, based on established standards. The importance of the convention extends to the human rights status granted to the theme of data protection[275].

However, even those Acts or instruments that do not explicitly refer to data protection principles (such as the Privacy Act of 1974[276] and the Fair Credit Reporting Act (FCRA) of 1970[277] in the USA, give effect to certain basic or core data protection

---

[272] Elaborated in 1980 and revised in 2013.
[273] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 193.
[274] LLOYD, Ian J. **Information Technology law**. 7 ed. OXFORD: Oxford University Press: 2014, p. 64
[275] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019, p. 195.
[276] 5 U.S.C § 552a. **The Privacy Act of 1974.** It is a federal law in the public sector. It was enacted to control the personal information practices of federal government agencies.
[277] The FCRA of 1970 is a federal law in the private sector and is specifically aimed at promoting fairness in credit reporting. 15 U.S.C. § 1681. **Commerce and Trade** § 1681. Congressional findings and statement of purpose**.**

principles.

The newly cited documents are not the only influences on data protection - other documents include, for example, the “United Nations Guidelines Concerning Computerized Personal Data Files” (1990) and the 'Safe Harbor Framework EUA-UE[278] issued by the U.S. Department of Commerce in July 2000.

Prior to the current General Data Protection Rule (GDPR), the European Union Data Protection Directive has been in force since 1998 as seen. This, in turn, required transfers of personal data to take place only to countries outside the European Union that provided an "adequate" level of privacy protection.

Understanding that U.S. law would not be considered appropriate for unrestricted flow with the European Union and to avoid the use of more complicated mechanisms for data transfers by US companies, the government negotiated an agreement to exempt European rules, applicable to this bilateral relationship.

Because there is an approach in the United States that combines legislation, regulations, and self-regulation, in a sectoral way, there were great difficulties in understanding what would be the "appropriate standard"[279]. The Commerce Department then led the purpose of "Principles" to provide a more predictable framework for the adequacy of data transfer and facilitate trade between the United States and the European Union.

Thus, from voluntary membership decision, to qualify as a member of the program, an organization could adhere to a self-regulatory privacy program that has already adhered to the requirements, or could develop the self-regulatory privacy program in accordance with the framework. In addition, compliance was monitored by the compliance with the seven Safe Harbor Privacy Principles, which are: notice; choice; onward transfer; access; security, and data integrity.

---

[278] U.S. DEP’T COM. **Welcome to the U.S.-EU Safe Harbor**. (Jan. 26, 2017, 12:38 PM), Available at: <http://2016.export.gov/safeharbor/eu/eg_main_018475.asp> [hereinafter Safe Harbor Overview] Accessed 04 Sep., 2021.

[279] U.S. DEP’T COM. **Welcome to the U.S.-EU Safe Harbor**. (Jan. 26, 2017, 12:38 PM), Available at: <http://2016.export.gov/safeharbor/eu/eg_main_018475.asp> [hereinafter Safe Harbor Overview] Accessed 04 Sep., 2021.

The seal generated by the "Safe Harbor Framework USA-EU" served as a presumption of compliance. However, the failure to renew certification, the distribution of misleading information about certification and, mainly, the difficulty of establishing surveillance mechanisms, led to questioning whether, in fact, the data were being protected or would be just a form of protectionism for companies. In an analysis made up to 2008, for example, only 348 of 1,109 organizations registered under Safe Harbor had minimally met the most basic compliance requirements[280].

In 2015, it was then overturned by the European Court of Justice, "in the wake of the revelation of U.S. government surveillance programs following public of classified material by former N.S.A. contractor Edward Snowden"[281].

It was from the General Data Protection Rule that in February 2016, a new self-regulatory model called the EU-U.S. Privacy Shield was agreed between the European Commission and the Department of Commerce, with the possibility of self-certification[282].

The issue also overflows with international law, and together with other elements, become true standards for data privacy protection by becoming models that have reached a transnational level.

From the American reality, Schwartz e Solove organized key Fair Information Practice Principles (FIPPs) that have proven to be enormously influential in the shaping of data privacy laws[283]. These principles on the one hand establish the duties and responsibilities of those who process personal data. On the other hand, it

---

[280] CONNOLLY, Chris. **The US Safe Harbor**: fact or fiction? 1, 4, 7 (2008), Available at: <http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf> Accessed 04 Sept., 2021.

[281] ALVAREZ, Daniel. **Safe Harbor is Dead**; long live the Privacy Shield? A.B.A., (May 20, 2016), Available at: <https://www.americanbar.org/groups/business-law/publications/blt/2016/05/09_alvarez/> Accessed 04 Sept., 2021.

[282] Recently, in Data Protection Commissioner v. Facebook Ireland Ltd (Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020), the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield, finding that U.S. surveillance laws do not afford EU data subjects adequate levels of protection under the European Union's Charter of Fundamental Rights (the "Charter") and General Data Protection Regulation (GDPR).

[283] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline.

describes the interests or rights that people have in relation to their data.

There is not a single authority (national, international, or transnational) responsible for determining what these principles are. On the contrary, there is a multiplicity of bases that led to the organization proposed by the authors. The generated document is part of the American law institute project and "seeks to move U.S. privacy law greater common ground and to close gaps in it"[284].

Some examples of the influence of the FIPPs can be found in U.S. federal laws such as the Fair Credit Reporting Act (1970), the Privacy Act (1974), the Video Privacy Protection Act (1988), the Health Insurance Portability and Accountability Act (1996), the Children's Online Privacy Protection Act (1998), and the Gramm-Leach-Bliley Act (1999). Also in state level, as the California Online Privacy Protection Act (2003) and the California Consumer Protection Act (2019)[285].

> At the international level, FIPPs have exercised a similar influence. The Organization for Economic Co-operation and Development (OECD) Guidelines of 1980 and 2013, the European Union Data Protection Directive of 1995, the EU Draft Data Protection Regulation of 2012, the EU General Data Protection Regulation of 2016, and the Asian-Pacific Economic Cooperation (APEC) Privacy Framework of 2004 all make recourse to the concept of FIPPs. Courts have also turned to the concept of FIPPs in different contexts to identify the responsibilities and liabilities of parties who process and share personal data[286].

The authors also remind that non-U.S. law is playing an increasingly important role within this country. U.S. companies have voluntarily adopted standards proposed by the GDPR as a form of belonging to global-data processing practices.

---

[284] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 2.

[285] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 3.

[286] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 3.

They called it “benchmark”[287], as a process of comparing products, services, and business practices. However, for the general objective of this work, this is the characterization of the standards.

That is, standards established in a transnational manner – without a state authority that demands, in which other forces appear as players of the business, and that generate a certain uniqueness beyond domestic or international law.

Therefore the principles listed here are treated as transnational. For these are not imposed by a single authority, and, on the contrary, they are a real mix of practices and debates that cross national borders to understand, in a transnational way, what data protection is about.

Thus, the central principles of data protection that can be identified will then be analyzed in their peculiarities. Important, however, to point out that not all appear exactly as formulated here, and that sometimes overlap not being possible to distinguish them clearly in a concrete situation.

The authors sought, however, a sense of uniformity between diverse sources, that “aim to develop concepts that can guide statutory law, the common law, other types of law, self-regulatory codes of best practices, and the organizational practices of private parties”[288].

These sources include privacy concepts from tort and contract law as well as the enforcement decisions of the Federal Trade Commission (FTC) and other regulatory agencies[289]. “In addition, and due to the significant influence of EU law on current FIPPs, at times, these Principles reflect concepts and terms developed by

---

[287] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 1.

[288] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 4.

[289] In particular, the FTC will be addressed as a standard source in the protection of children's data from the YouTube case dealt with in the chapter 7.

and incorporated in EU and other non-U.S"[290], which provides for the harmonization of principles beyond national law on the following bases[291]:

The authors' analysis will be commented and sometimes complemented with Brazilian legislation, when relevant. However, in the chapter 5, the principles listed will be related to Brazilian legislation (LGPD).

The basis of the comparison FIPPs analyzed by the authors included: HEW - Code of Fair Information Practices (1973)[292]; OECD - Privacy Principles (1980)[293]; APEC - Privacy Framework (2005)[294]; DHS – Fair Information Practice Principles (2008)[295]; White House – Consumer Privacy Bill of Rights (2012)[296]; FTC - Privacy Frame-work and Impl. R., (2012)[297]; Privacy Act (1974)[298]; HIPAA (1996)[299]; Gramm-Leach-Bliley Act (1999)[300]; PIPEDA (Schedule 1) (2000)[301]; EU Directive - EU Data Protection Directive (1995)[302]; EU Regulation – EU General Data Protection

---

[290] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 4.

[291] The description of the subitems will take place from the systematization brought by the authors in the aforementioned work, unless otherwise referenced.

[292] The Code of Fair Information Practices of the Department of Health, Education and Welfare represents the first articulation of FIPPs. http:/ericorg/hrivacv/consumer/code

[293] As privacy law continued to evolve, the OECD, a group of 33 leading industrial countries concerned with global economics and development, proposed their influential OECD Privacy Principles http://oecdprivacy.org

[294] APEC, an organization of 21 Pacific Rim countries, introduced FIPPs in order to enable multinational businesses to implement uniform approaches to the use of personal data. The resulting guidelines strongly reflect the OECD Privacy Principles.

[295] The Privacy Office at the Department of Homeland Security's FIPPs resemble the OECD Privacy Principles as well.

[296] The Consumer Privacy Bill of Rights published by the White House aims to apply comprehensive and globally recognized FIPPs for purposes of consumer protection.

[297] Recently, the Federal Trade Commission issued a major report about privacy, which also included FIPPs.

[298] Among the early statutes that include FIPPs is the Privacy Act. It regulates the collection, use, and disclosure of personal data by federal agencies. (5 U.S.C § 552a)

[299] Pursuant to HIPAA, the Department of Health and Human Services promulgated regulations of the privacy and security of medical information. (45 C.F.R §§ 160, 162, 164)

[300] The GLB Act's seeks both to facilitate data sharing among financial institutions and their affiliates and to protect customer privacy. It contains FIPPs as well. (15 U.S.C § 6801 et seq., 16 C.F.R §§ 313, 314)

[301] PIPEDA is a Canadian privacy statute that regulates all private-sector entities that collect personal information on Canadians and personal information used in connection with any commercial activity.

[302] The EU Data Protection Directive's goal is to facilitate the free flow of personal information within the EU by establishing an equally high privacy level in all Member States. It is not directly binding, but

Regulation (2016)[303]; NAI Principles (Section III) (2008)[304]; AICPA/CICA GAPP (2009)[305]; DAA Self-Regulatory Principles for OAB (2009)[306] and GSMA Mobile Privacy Principles (2012)[307].

The sub-items in this topic will be based on a summary of the main analyses of the document generated by Schwartz and Solove at The American Law Institute, and therefore will not be referenced unless other sources overlap the analysis[308].

4.1 Transparency statement

Transparency statement assumes that every data controller should give publicity in an accessible, clear, conspicuous, and accurately way of their activities.

Some peculiarities should be observed. Confidential information, such as industrial secrets, is excluded from this need to provide information. Proportionality is also evidenced between the sophistication of transparency and the security risks of the committed activity.

And access to information (another principle that overlaps with transparency) must be such that current and previous information must be preserved for the reasonable access of those who are interested.

---

implemented on the national level by each country.

[303] The EU General Data Protection Regulation is the proposed successor to the EU Data Protection Directive. It seeks to update privacy law within the EU with a single law that will be immediately binding on all EU member states.

[304] The Network Advertising Initiative (NAI), an industry trade group, develops self-regulatory standards for online advertising, among which are the NAI Principles.

[305] The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed a set of FIPPs to be used by companies in their self-regulation of privacy.

[306] The Digital Advertising Alliance (DAA) is an organization that provides a self-regulatory FIPPs regime for interest-based advertising.

[307] The GSMA is an association of mobile operators and related companies devoted to supporting the standardization, deployment, and promotion of the GSM mobile telephone system. It also released a self-regulatory framework containing FIPPs.

[308] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline.

In practice, transparency is based on public knowledge of the database, prior authorization of operation, or notification to an authority of its existence.

Transparency also appears as publicity, Openness or Education in different sources:

- There must be no personal data record-keeping systems whose very existence is secret.[309]

- 6. There should be a general policy of openness about developments, practices and policies with respect to personal data[310].

- Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII)[311].

- 2. Consumers have a right to (…) information about privacy and security practices. (…) [C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it (…) [and further information][312].

- Transparency Baseline Principle: "Companies should increase the transparency of their data practices." C. Final Principle: "All stakeholders should expand their efforts to educate consumers"[313]

- (e) "Each agency that maintains a system of records shall (…) (4) (…) publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records".[314]

---

[309] HEW – The Code of Fair Information Practices (1973).
[310] OECD – Privacy Principles (1980).
[311] DHS – Fair Information Practice Principles (2008).
[312] THE WHITE HOUSE – Consumer Privacy Bill of Rights (2012)
[313] FTC – Privacy Framework and Implementation Recommendation (2012).
[314] Privacy Act (5 USC § 552a) (1974)

- 4.8 Principle 8: 4.8.1 "Organizations shall be open, about their policies and practices with respect to the management of personal information." 4.8.2 "The information made available shall include (a) [contact details to inquire about policies and practices], (b) the means of gaining access to personal information (…) [and further information]."[315]

Transparency statements are dynamic when informing the public about an entity's policies and practices. These transparency data can also reveal the trends of the sector and influence them. This influence can also happen within entities in the way controllers or data processors articulate their processes.

It differs, therefore, from the individual notice that it plays a mainly static role in choosing between products and services based on the privacy policy of different entities, as will be seen below.

4.2 Individual Notice

Individual notice is a document distinct from the transparency statement required and must be provided every time a controller engages in an activity with personally identifiable information.

The purpose is to inform people how personal information is being collected, processed, and used so that an informed decision can be made.

The main characteristics to be observed is that this notice should be reasonably practicable, considering the capabilities of those who operate them. In addition, it should be reasonably accessible, provided at na appropriate time, clear, intelligible, inform the nature of the data activity, the uses made of the data, the interests implicated, and how the data subject may exercise such interests.

Should also inform about the legal rights pertaining to the situation and a

---

[315] PIPEDA (Schedule 1) (2000)

contact so that the user can send questions or complaints.

There are specific situations in which they would require heightened notice with additional requirements, as in significant risk or unexpected data activity (something that a reasonable person would not expect based on the context of personal-data activities).

Most privacy laws have the notice requirements mandatory, making this characteristic of inalienability, as The Gramm-Leach-Bliley Act 18 that requires financial institutions to supply consumers with notices that explain these companies' privacy practices[316].

Or, as found in different sources:

- II. Personal Information controllers should provide (…) statements about their practices and policies that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; (…) [and further information][317].

- § 164.520(a)(1) "[Subject to exceptions], an individual has a right to adequate notice of the uses and disclosures of protected health information (…), and of the individual's rights and the covered entity's legal duties (…)". (Details in § 164.520(b)). § 164.530(i)(1) "A covered entity must implement policies and procedures with respect to protected health information".[318]

- A Final Principle: "Privacy notices should be clearer, shorter, and more standardized ..."[319]
- Art. 10: "[T]he controller or his representative must provide a data

[316] Gramm-Leach-Bliley Act, 15 U.S.C. § 6803 (2012).
[317] APEC – Privacy Framework (2005).
[318] HIPAA (45 CFR §§ 160, 162, 164) (1996).
[319] FTC – Privacy Framework and Implementation Recommendation (2012).

subject (…) with at least the following information ... (a) the identity of the controller (…); (b) the purposes of the processing (…); (c) (…) further information (…)". (See Art. 11 for the case where information was not obtained from the data subject.)[320]

- Art. 12: 1. "The controller shall take appropriate measures to provide (…) information [about data processing] ... in a concise, transparent and easily accessible form. Art. 13: 1."[It shall] provide the data subject with the following information: (a) the identity (...) of the controller; (b) the contact details of the data protection officer; [and further information]." (See also Art. 14.)[321]

As explained in the previous topic, transparency statement principles often overlap with individual notice. The division between them is only a didactic way of presenting them in their unique characteristics, not denying, however, their convergences.

4.3 Consent

The main connection between this principle and the previous one is that no consent is valid if there is not, in advance, reasonable individual notice. That is, the individual must have received sufficiently clear, accurate, and accessible information so that he can make an informed choice about consent.

Consent also appears in several sources such as "authorization" or "notice and choice":

- Privacy Act prohibits the disclosure of records without the "consent" of the individual[322];
- Health Insurance Portability and Accountability Act (HIPAA) states

---

[320] EU Data Protection Directive (1995)
[321] EU General Data Protection Regulation (2016)
[322] 5 U.S.C. § 552a(b),

that protected health data cannot be disclosed without "authorization"[323];

- In the context of the disclosure of consumers' location information to third 24 parties, the FTC calls for "more prominent notice and choices"[324].

According to Article 5, item XII of the LGPD, the consent of the data subject must be a free, informed, and unequivocal manifestation, as a reflection of the GDPR definition[325].

As an additional restriction, consent can be withdrawn at any time and cannot avail itself of inaction or silence. That is, it must be expressed by the holder in some way.

The collection of child data also requires special consent requirements, as will be addressed in the following chapters.

Consent in U.S. data protection laws appears in a binary logic as opt-in and opt-out systems. In the opt-in the data subject prior consents in an expressly way, accepting each form of use of your data. On the other hand, the subsequent choice, even implicitly extracted, consists of the opt-out[326].

In the California Privacy Act[327], for example, businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, subject to certain defenses. Must include a "Do Not Sell My Personal Information" link in a clear and conspicuous location on a website homepage. Must not request reauthorization to sell a consumer's personal information for at least 12

---

[323] 45 C.F.R. § 164.508(a)(1).
[324] FEDERAL TRADE COMMISSION. **Protecting Consumer Privacy in an Era of Rapid Chang**e: Recommendations For Businesses and Policymakers. March, 2012. Available at: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> Accessed 03 Mar., 2021.
[325] any freely given specific, informed and unambiguous indication of the data subject's 28 wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to 29 the processing of data relating to him or her. EU General Data Protection Regulation, Article 4(11).
[326] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 233-235.
[327] Cal. Civ. Code §§ 1798.120 and 1798.135(a)-(b).

months after the person opts-out.

The LGPD, on the other hand, does not include a specific right to opt-out of personal data sales. Only if consent is required, and there were changes in the purpose for the processing of personal data not compatible with the original consent, the controller must inform the holder in advance about the changes of purpose, and the holder may revoke the consent if he disagrees with the changes.

According to Bioni[328], consent becomes a major concern of data protection and a regulatory guideline to determine whether the processing of personal data is fair and lawful.

Consent establishes control over the citizen over his/her personal data as a synonym for informational self-determination. The principle makes clear the elevation of the holder of personal data as

> the main actor in the normative dynamics on the protection of personal data. The replication of many of the above rights listed in the most diverse laws, that converge to the prominent role that the consent of the data subject plays in this normative arrangement, is enlightening to understand how to date the norms under such a theme have been structured around the world[329]

However, there is the caveat that new technologies increase the difficulty of understanding individuals so that one can, in fact, make choices about their personal uses[330], especially regarding the disparity of forces, typical of the consumer contracts.

Other points such as: whether it would be possible, really, consent to be free; the lack of clarification; lack of choice; manipulation for obtaining; the burden given to consent; as well as the asymmetry and (hyper)vulnerability of the scope of personal data protection can make it extremely fragile.

Consent is not the object of research, and specific situations regarding the

---

[328] BIONI, Bruno Ricardo. **Protection of personal data**: the function and limits of consent. Rio de Janeiro: Forensics, 2019, p. 175-176.
[329] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 176.
[330] The OECD Privacy Framework 2013. **The evolving privacy landscape**: years after the OECD Privacy Guidelines (2011), p. 67-68. Available at: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Accessed 15 Mar., 2021.

relationship with child data protection will be addressed in the relevant chapter. However, it is important to note that consent will not be interpreted as synonymous with autonomy of will.

4.4 Confidentiality

The Duty of confidentiality exists “whenever personal data is collected under and express or implied promise of confidentiality or a legal obligation of confidentiality”, or “based on ethical standards, such as professional rules of conduct, or applicable law”[331].

Relationships as a doctor-patient are a classic example of the confidentialness required by the category, which extends to hospitals, therapists, insurance companies, banks, accountants, and lawyers, among other professionals.

Regardless of whether there is a consent form, information collected in certain circumstances of trust holds an expectation on the part of the data subject that it is confidential. And so, they should be.

Several practical cases address this theme and the implication of "expectation of privacy", as pointed out in the first chapter. This is therefore information that approaches intimacy or secrecy, as a more sensitive part of personal data and that must remain in seclusion.

4.5 Use Limitation

The use limitation is based on the notice and consent for a given data activity. That is, the data should be limited to the accuracy of what was previously

---

[331] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 56.

proposed and agreed upon.

There are limited exceptions, when, for example, when use is required by law; or obtaining consent would be impractical, impermissible under law, too costly or, difficult.

Minimization, another principle listed by some authors, differs because it limits the use to the relevance and needs to use certain data for what was specified in the purpose of collection. While the limitation of use somewhat extends this list, it does not use the criterion of relevance or need but does ensure that the use is limited to the science of the data subject. They appear as follows:

- 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent[332].
- 2. Personal data should be relevant to the purposes for which they are to be used (…); 3. Use of personal data should be] limited to the fulfillment of those purposes [for which they were collected] or such others as are not incompatible with those purposes (...)[333].
- lll. The collection of personal information should be limited to information that is relevant to the purposes of collection (…); IV. Subject to consent and other exceptions personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes[334].
- Purpose Specification: DHS should (…) articulate the purpose or purposes for which the Pll is intended to be used. Data Minimization: DHS should only collect Pll that is directly relevant and necessary to accomplish the specified purpose(s). Use

[332] HEW – The Code of Fair Information practices (1973)
[333] OECD – Privacy Principles (1980)
[334] APEC – Privacy Framework (2005)

Limitation: DHS should use PII solely for the purpose(s) specified in the notice[335].

- 3. Companies should limit (…) use and disclosure (…) to (...)purposes (…) consistent with (…) the consumer [relationship] and the [disclosure] context (…); 6. Companies should collect only as much personal data as they need to accomplish the purposes specified [at 3.][336].

- Simplified Consumer Choice - B. Final Principle: Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes[337].

- (e) "Each agency (…) shall (1) maintain (…) only such information (…) as is relevant and necessary (…); (3) inform each individual (…) (B) [of] the (…) purpose (…) for which the information is intended to be used; (…) [and] (11) (…) publish in the Federal Register notice of any new use (…)[338].

- 164.502(b) When using or Disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." (See also § 164.514(d))[339].

- § 6802(c) "[N]onaffiliated third parties receiving (…) information (…) shall not (…) disclose [those] to [other] nonaffiliated third parties; §

---

[335] DHS – Fair Information Practice Principles (2008)
[336] THE WHITE HOUSE – Consumer Privacy Bill of Rights (2012)
[337] FTC – Privacy Framework and Implementation Recommendation (2012)
[338] Privacy Act (5 USC § 552a) (1974)
[339] HIPAA (45 CFR §§ 160, 162, 164) (1996)

6802(d) "[Subject to exceptions, a] financial institution shall not disclose (…) an account number or similar [financial information] to any nonaffiliated third party for [marketing use]."(For details, see 16 CFR § 313.10 et seq.) [340].

- 4.2 Principle 2: The [collection] purposes (…) shall be identified (…)at or before the time [of collection]; 4.4 Principle 4: The collection (…) shall be limited to (…) the purposes identified by the organization; 4.5 Principle 5: Subject to exceptions, personal information shall not be used or disclosed for (…) other than [collection purposes] (…)[341].

- Art. 6: 1. Personal data must be: (…) (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[342].

- Art. 5: Personal data shall be: (…) (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and limited to what is necessary in relation to the purposes (…)"[343]

As seen above, the GDPR provides the regulation of the secondary use of data, in addition to the primarily requested, based on the principle of data minimization, requiring that personal data be adequate, relevant, and limited to what is necessary.

The "legitimate interest", which appears in Article 6, as the legal basis for the processing of personal data in the GDPR has much convergence with the "use

---

[340] Gramm-Leach-Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)
[341] PIPEDA (Schedule 1) (2000)
[342] EU Data Protection Directive (1995)
[343] EU General Data Protection Regulation (2016)

limitation" here. Nevertheless,

> a key difference is that the legitimate-interest exception to the Principles is narrower, as secondary use is more highly regulated than initial primary use. Another difference is that the Principles recognize an exception for uses that significantly advance protection against criminal or tortious activity conducted by the individual whose personal data is involved[344].

Brazilian legislation incorporated the legitimate interest in Art. 10 of the LGPD, also as a legal basis source for the processing of data. In addition, information on the use of data (individual notice) must contain the specific purpose of the processing, and therefore limit the use to the consent given (art. 5º, XII, LGPD).

4.6 Access and Correction

Considered by the authors[345] as one of the most universally accepted Fair Information Practice Principles, access and correction are guaranteed by most statutes and regulations.

It begins with the right of the data subject to confirm the existence of personal data in the hands of a particular entity, through the right of access to such data until, finally, the possible correction, or even deletion of that data.

This whole process is guaranteed in different ways, depending on the source:

- 2. There must be a way for a person to find out what information about the person is in a record and how it is used; 4. There must be a way for a person to correct or amend a record of identifiable

---

[344] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 63.

[345] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 68.

information about the person[346].

- 7. An individual should have the right: a) to obtain from a data controller (…) confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him (…) ; (…) d) to challenge data relating to him and ... to have the data erased, rectified, completed or amended[347].

- VIII. Individuals should be able to: a) obtain (…) confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them (…) personal information about them; (…) and, c) challenge [their] accuracy (…) [and] have the information rectified, completed, amended or deleted[348].

- Individual Participation: DHS should (…) provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PL[349]

- 5. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate[350].

- Transparency B. Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use[351].

---

[346] HEW – The Code of Fair Information practices (1973)
[347] OECD – Privacy Principles (1980)
[348] APEC – Privacy Framework (2005)
[349] DHS -Fair Information Practice Principles (2008)
[350] THE WHITE HOUSE – Consumer Privacy Bill of Rights (2012)
[351] FTC – Privacy Framework and Implementation Recommendation (2012)

- (c) "[Subject to exceptions, each agency (…) shall (…) (3) (…) make [an accounting of disclosures] available to the individual named in the record (…); and (4) inform any person (…) about any correction (…); (d) Each agency (…) shall (1) [permit an] individual (…) to review the record (…); (2) permit the individual to request amendment of a record(…)[352].

- § 164.524(a)(1) Subject to exceptions, an individual has a right of access to inspect and obtain a copy of protected health information (…); § 164.526(a)(1) An individual has the right to have a covered entity amend protected health information(…)[353].

- 4.9 Principle 9: Upon request, an individual (…) shall be given access to [collected] information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate[354].

- Art. 12: Member States shall guarantee every data subject the right to obtain from the controller: (a) (…) confirmation as to whether or not data relating to him are being processed and information (…) [as] to whom the data are disclosed, communication to him (…) of the data (…) and of any available information as to their source (…) (b) as appropriate the rectification, erasure or blocking of data (…)[355].

- Art. 15: 1. The data subject shall have the right to obtain (…) confirmation as to whether (…) her [data] are being processed (…) 3. The controller shall provide (…) [the] data (…); Art. 16: The data subject shall have the right to obtain (…) rectification (…) [and completion of] personal data (…); Art 17: 1. The data subject shall

[352] Privacy Act (5 USC § 552a) (1974)
[353] HIPAA (45 CFR §§ 160, 162, 164) (1996)
[354] PIPEDA (Schedule 1) (2000)
[355] EU Data Protection Directive (1995)

> have the right to (…) erasure of [her] data (…); Art. 18: "The data subject shall have the right to (…)restriction of processing [when certain requirements are met](…)[356].

The LGPD brings, as well as the GDPR and PIPEDA, a greater scope to the principle than in U.S. legislation. It ensures free and facilitated access to the holders on the completeness of their personal data (Art. 6, IV), as well as the correction of incomplete, inaccurate, or outdated data (art. 18, III).

4.7 Data Portability

The data portability predicts that the controller provides to the data subject a copy of his or her personal data in a usable format, that can be used in other platforms or situations.

It is generally limited to information collected from the data subject by the organization and excludes data concerning the business methods and internal operations of data processors.

Because U.S. data protection laws are largely sectorized, the data portability appears in different situations, such as in The Communications Act of 1934[357], by which portability of the phone number to another carrier is allowed. Furthermore, health information appears in HIPPA with guaranteed portability in a "designated record set"[358].

Other projects seek to establish general parameters for data portability, such as an initiative led by tech companies, including Apple, Microsoft, Google, Twitter, and Facebook, called "Data Transfer Project" (DTP). This is an “open-source,

---

[356] EU General Data Protection Regulation (2016)
[357] 47 U.S.C. § 251(b)(2). Federal Communication Commission (FCC) define number portability as "the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another." 47 U.S.C. § 153(37); 47 C.F.R. § 52.21(n).
[358] 45 C.F.R. § 164.524

service-to-service data portability platform so that all individuals across the web could easily move their data between online service providers whenever they want"[359].

This example is especially relevant because it confirms the transnationality characteristic of data protection principles. In this particular situation, it is not the state, but it is the big players who have determined the rules of the game that will influence the lives of millions of users.

The GDPR[360], as well as the LGPD[361] explicitly bring the right of the data subject to portability to another supplier.

2.3.8 Data Retention and Destruction

Data retention and destruction are equally important security measures to safeguard the interests of those involved. Retained data presents risks of loss, or leakage, for example. On the other hand, destroying all data is unfeasible for compliance with terminated legal obligations and other expected exceptions, which include scientific or historical research.

Just as important as the ability to retain information is to storage or delete it. The idea of this principle is that all data, after completing its purpose, must be retained (filed) or deleted, depending on the case.

And as simple as it may seem, data destruction is a complex task in the digital world and often requires elaborate technical capacity in addition to an efficient policy of good practices.

These are technical criteria that drive the principle and create the necessary protection standards. One example is the National Institute of Standards

---

[359] **Data Transfer Project**. Available at: <https://datatransferproject.dev/>Accessed 03 Mar., 2022.
[360] Art. 20: 2. "The data subject shall have the right to receive the personal data concerning... [her and] to transmit those data to another controller without hindrance
[361] Art. 18. The holder of the personal data is entitled (...), at any time and upon request: (...) V - data portability to another service provider or product, (...)

and Technologies, which provides, through the Guidelines for Media Sanitization[362], reference points for an organization to develop data retention and destruction procedures, based on four categories: disposal, clearing, purging, and destroying.

Issues such as the reasonable time lapse for data to be forwarded to retention or destruction; requirements for a policy of procedures for this; as well as data mapping, while inventory of personal data that the organization has (even as a requirement for accountability); and data protection for future litigation are issues sensitive to this principle.

Citations in guidelines or frameworks overlap with previous principles, as often the right to delete data comes along with access and correction of data. What is considered is how and even when this data is available to the user.

As in the case of the GDPR, which contains an individual right to deletion (art. 17), or the LGPD which mentions in art. 18 the right of the data subject the "VI - deletion of personal data processed with the consent of the data subject"[363]. In the same way, the California Data Protection Act provides: “§ 1798.105(a) A consumer shall have the right to request that a business delete any personal information about the consumer the business has collected from the consumer”[364].

At least 34 U.S. states have data-destruction laws[365]. Still, because it has

---

[362] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines for Media Sanitization**. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf> Acessed 02 May, 2022.

[363] LGPD - General Data Protection Law (2018).

[364] California Consumer Privacy Act of 2018,

[365] **Alabama** (Ala. Code § 8-38-10); **Alaska** (Alaska Stat. § 45.48.500 et seq.); **Arizona** (Ariz. Rev. Stat. § 44-7601); **Arkansas** (Ark. Code §§ 4-110-103, -104); **California** (Cal. Civ. Code §§ 1798.81, 1798.81.5, 1798.84); **Colorado** (Colo. Rev. Stat. § 6-1-713); **Connecticut** (Conn. Gen. Stat. § 42-471); **Delaware** (Del. Code tit. 6 § 5001C to -5004C, Del. Code tit. 19 § 736); **Florida** (Fla. Stat. § 501.171(8)); **Georgia** (Ga. Code § 10-15-2); **Hawaii** (Haw. Rev. Stat. §§ 487R-1, 487R-2, 487R-3, Haw. Rev. Stat. § 261-17.7(d), Haw. Rev. Stat. § 52D-14(c) 3); **Illinois** (20 ILCS 450/20, 815 ILCS 530/30, 815 ILCS 530/40); **Indiana** (Ind. Code §§ 24-4-14-8, 24-4.9-3-3.5(d)); **Kansas** (Kan. Stat. § 50-6, 139b(2)); **Kentucky** (Ky. Rev. Stat. § 365.725); **Louisiana** (La. R.S. 51:3074(B); **Maryland** (Md. Com. Law § 14-3502, Md. State Govt. Code § 10-1303); **Massachusetts** (Mass. Gen. Laws Ch. 93I, § 2); **Michigan** (MCL § 445.72a); **Montana** (Mont. Code Ann. § 30-14-1703); **Nebraska** (Neb. Rev. Stat. § 87-808(1); **Nevada** (Nev. Rev. Stat. § 603A.200); **New Jersey** (N.J. Stat. § 56:8-161, -162); New Mexico (N.M. Stat.§ 57-12C-3); **New York** (N.Y. Gen. Bus. Law § 399-H); **North Carolina** (N.C. Gen. Stat. § 75-64); Oregon (Ore. Rev. Stat. § 646A.622); **Rhode Island** (R.I. Gen. Laws § 6-52-2); **South**

many peculiarities, it also covers a range of sectoral-specific laws in the federal and state levelsthe in the United States[366].

4.8 Data Security

Data security measures are one of the major concerns of frameworks and statutes, which cover, in general, safeguards against foreseeable risks, including unauthorized access, acquisition, use, modification, sharing or destruction of personal data, as seen:

- 5. Any organization (…) must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data[367].
- 5. Personal data should be protected by reasonable security safeguards (…)[368].
- I. [I]nformation protection should (…) prevent the misuse of [personal information (…) [It] should take account of [the] risk [of misuse] (…); VII. [I]nformation controllers should protect personal information (…) with appropriate safeguards (…) Such safeguards should be proportional (…)[369].
- Data Minimization: DHS should only (…) retain PII for as long as necessary to fulfill the specified purpose(s). PII should be disposed

---

Carolina (S.C. Code § 37-20-190, S.C. Code 30-2-310); **Tennessee** (Tenn. Code § 39-14-150(g)); **Texas** (Tex. Bus. & Com. Code § 72.004, § 521.052); **Utah** (Utah Code § 13-44-201); **Vermont** (9 Vt. Stat. § 2445); **Virginia** (Va. Code § 2.2-2009 (F)); **Washington** (Wash. Rev. Code § 19.215.020) and **Wisconsin** (Wisc. Stat. § 134.97).

366 SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 81.

367 HEW – The Code of Fair Information practices (1973)

368 OECD – Privacy Principles (1980)

369 APEC – Privacy Framework (2005)

of in accordance with DHS records Disposition schedules (…); Security: DHS should protect PII (…) through appropriate security safeguards against risks (…)[370].

- 4. Consumers have a right to secure and responsible handling of personal data. Companies should assess the (…) risks associated with their personal data practices and maintain reasonable safeguards to control risks (…); 6. Companies should securely dispose of or deidentify personal data once they no longer need it[371].

- Privacy by Design A. Final Principle: Companies should incorporate substantive Privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices (…)[372].

- (c) Subject to exceptions, each agency ... shall ... (2) retain [an] accounting [of disclosures] (…) (e) "Each agency (…) shall (…) (10) Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records (…)[373].

- § 164.530(c)(1) A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." (See generally § 164.302 et seq.)[374].

- 16 CFR § 314.3(a) [Financial institutions] shall develop, implement, and maintain a comprehensive information security program ." (See

---

[370] DHS – Fair Information Practice Principles (2008)
[371] THE WHITE HOUSE – Consumer Privacy Bill of Rights (2012)
[372] FTC – Privacy Framework and Implementation Recommendation (2012)
[373] Privacy Act (5 USC § 552a) (1974)
[374] HIPAA (45 CFR §§ 160, 162, 164) (1996)

all details in 16 CFR § 314)[375].

- 4.7 Principle 7: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. 4.7.3 The methods of protection should include (a) physical (…) ;(b) organizational (…) and (c) technological measures (…)[376].

- Art. 17: 1. [T]he controller must implement appropriate technical and organizational measures to protect personal data (…) [S]uch measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[377].

- Art. 32: 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (…)[378].

All other principles, even if they were respected, loses control if the data are leaked, erroneously deleted, or tampered with. Concern for the integrity and security of this information is, as seen, central in most frameworks and statutes concerning data privacy.

It is interesting to note that, as in other principles, different legal bases converge in the scope of protection and concerns regarding data protection/privacy.

---

[375] Gramm-Leach-Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)
[376] PIPEDA (Schedule 1) (2000)
[377] EU Data Protection Directive (1995)
[378] EU General Data Protection Regulation (2016)

4.9 Onward Transfer

The principle of Onward Transfer aim to prevent personal data from falling outside of its protective bubble when data is transferred along a chain of entities.

For this reason, it is also overlaid with the other principles, because the transfer, as well as the initial collection, must comply with all the criteria already provided for, since the transparency statement, individual notice, consent, confidentiality, access and correction, data portability, data security,

As an example, Article 28 of the GDPR, imposes duties on controllers that contract with data recipients-called "processors". As in:

- 4.1. Principle 1: 4.1.3 An organization is responsible for Personal information in its possession (…) Including information (…) transferred to a third party (…)[379].
- § 6802(c) Nonaffiliated third parties receiving] (…) information (…) shall not (…) disclose [those] to [other] nonaffiliated third parties; § 6802(d)
- "[Subject to exceptions, a] financial institution shall not disclose (…) an account number or similar [financial information] to any nonaffiliated third party for [marketing use] (For details, see 16 CFR § 313.10 et seq.)[380].

The Brazilian LGPD, when dealing with child data, details that data collected from children for the purpose of contact with parents or legal guardians, can be used only once, cannot be stored, nor transferred to third parties[381].

---

[379] PIPEDA (Schedule 1) (2000)
[380] Gramm-Leach-Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)
[381] Art. 14, § 3º, LGPD.

4.10 Accountability and enforcement

In addition to the above principles, accountability and enforcement are other common elements that surround data protection at the transnational level.

Briefly, it is anticipated that data controllers and processors will be responsible for complying with data protection standards, and therefore assess the risks of their activities related to data privacy and security.

To do so, a reasonable privacy program is required, appropriate to the size, complexity and resources of the company, as well as the amount of data processed.

It is also essential that there are express and clear security procedures and policies; inventory of the data processed in a manner compatible with the previous principles; training programs; among other measures that help the company comply with the established requirements.

The concepts of “privacy and security by design and by default” are still in the Accountability topic. Being privacy and security by design:

> (1) A data controller or data processor shall analyze the privacy and security implications early on in the development of any new product, service, or process. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented.
>
> (2) A data controller or data processor shall examine how the product, service, or process should be designed to address the privacy or security issues identified in the analysis. The outcome of this examination shall be reflected in the final design of the product, service, or process. Reasonable design choices shall be made. Design choices and the reasoning that supports them shall be documented[382].

While Privacy and security by default, means that:

---

[382] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 182.

> 1) A data controller or data processor shall analyze the default settings of any existing or new product or service and how such settings implicate privacy and security. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented and repeated at reasonable intervals.
>
> (2) A data controller or data processor shall draw on the outcome of this examination in the final default-setting choices that are made. Reasonable defaultsetting choices shall be made. Default-setting choices and the reasoning that supports them shall be documented[383].

That is, “privacy by default” means that the “privacy by design” principle should be incorporated by default into any system or business, so that personal data is automatically protected without any action from the data subject.

Moving on to the issue of enforcement, it is necessary that the law recognizes the principles set out here so it could have effectiveness the desired protection.

Enforcement mechanisms also include individual and collective measures of judicial protection that take into account, when there is a violation of a principle, the responsibilities of those involved, the severity of the event, guilt, the unjust enrichment, among other possible criteria that compensate for the unlawful or unauthorized use the personal data[384].

Finally, the principles listed in the sub-items will be again addressed and correlated with the General Data Protection Law in Chapter 5, as well as the general foundation of transnational privacy protection criteria to children's data in the final chapter.

---

[383] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 183.

[384] SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline, p. 184.

CHAPTER 5
PROTECTION OF CHILDREN'S DATA IN BRAZIL

Data protection and child privacy in Brazil is specifically provided for in the General Data Protection Law (LGPD), which is cross-cutting through different economic agents (private, public, academic and third sector).

During almost eight years of discussion to reach the outcome of this law, the European Union's General Data Protection Regulation (GDPR) was also under discussion. Due to its influence on the LGPD, it can be said that Brazilian legislation was inspired by the product of European regulations, but with peculiarities in its details.

These peculiarities are not only found in the literal text of the norm, but in its interpretation from the legal system of each place. In particular, as data protection, it is concerned with the systematic interpretation with the Statute of the Child and Adolescent (ECA).

Regarding the use of data for commercial purposes, with an advertising focus, the Consumer Protection Code and CONAR's Advertising Self-Regulation Code should also be considered.

Thus, this item will study the LGPD from the interpretation dialogued with other sources of domestic law in their individualities, as well as the interconnections between them in order to understand, broadly, how data protection and child privacy is protected by the Brazilian legal system.

5.1 LGPD comprehensiveness

5.1.1 Who is protected

The General Data Protection Act applies to any processing operation carried out by a natural person or by a legal entity under public or private law,

regardless of the means used, the country of its headquarter, or the country where the data are located, since: (i) the processing operation is carried out in the national territory; (ii) the purpose of the processing activity is to offer or supply goods or services or the processing of data from individuals located in the national territory; or (iii) the personal data subject to the processing have been collected in the national territory[385].

The LGPD does not bring its own definition for children. It is considered, then, the concept brought by the Statute of the Child and Adolescent, as a person up to 12 years old incomplete[386].

The European Union, for example, considers 16 years, but allows member countries to reduce up to 13 according to their internal laws (art. 8, GDPR).

Similarly, as will be seen in the next subchapter, U.S. federal child protection legislation has limited the 13-year-old as a parameter. What, in practice, ends up being admitted as the age limit of childhood by those who somehow treat data.

That is, there is an age difference that can create a vacuum of protection for children by the LGPD of at least one year, compared to external standards.

5.1.2 Which data is contemplated

LGDP provides for the processing of personal data, including, but not exclusively, in digital media. For the law, personal data means all "information relating to identified or identifiable natural person"[387].

Therefore, the concept of "personal data" is not restricted to identity documents, addresses or photos. On the contrary, it covers all the pieces of information that may be linked to the person, such as pages browsed on the internet, photos liked on the social network or the time of use of a particular application. That

---

[385] Art. 3º, caput, I and III, LGPD.
[386] Art. 2º, ECA.
[387] Art. 5º, I, LGPD.

is, everything that could be monitored and tracked to make up the profile of a specific person (identified) or that could identify one (identifiable).

It applies to all companies, which act online or offline, whether public or private. It applies to those who collect data for commercial purposes and also by the public administration “for the processing and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments[...][388]”.

"Non-personal" data are excluded from their direct competence, such as:

> (...) corporate data, confidential or confidential documents, business secrets, strategic plans, algorithms, formulas, software, patents, among other documents or information that are not related to the identified or identifiable natural person[389] (free translation).

The law also does not protect anonymized data, as those that in its origin were personal, but were unrelated to the attributes that allowed identification[390]. For example, a statistical value generated from the consumption profile of a particular product in the supermarket. Initially, the purchase registration is obtained, with payment method, perhaps the name or some identification document among other data that may be personal to that consumer. From the moment this data becomes only a large statistical index, without direct linkage to the person, it becomes anonymized. Thus, knowing that 20% of consumers of this product buy it again in the following month is not a personal data, but an anonymized data.

Personal data held by natural persons that are not intended for economic purposes[391] or those carried out exclusively for journalistic or academic purposes are also excluded from the application of this standard. Therefore, the data collected exclusively to manage the grades of students in a school is not contemplated by law, however, when using this information to offer an extracurricular course, the commercial purpose is born, and consequently will be covered by the determination

---

[388] Art. 7º, III, LGPD.
[389] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD**: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 19.
[390] Art. 5º, III.
[391] Art. 4º, I, LGPD.

of the specific law[392].

Another category excluded from the scope of the LGPD is state data carried out for exclusive purposes of public security, national defense, state security or investigation and prosecution of criminal offences[393].

Finally, there is still territorial restriction. For the application of the LGPD, the data must necessarily be processed in national territory[394].

As “processing”, it is understood all operation carried out with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination, or extraction[395].

5.2 Legal fundamentals or regulatory frameworks

The LGPD contemplates data protection through the basis of respect for privacy, of informative self-determination, freedom of expression, information, communication and opinion, the inviolability of intimacy, honor and image, economic and technological development and innovation, free initiative, free competition and consumer protection, human rights, the free development of personality, dignity and the exercise of citizenship by natural persons[396].

The activities of processing personal data should observe the principles listed in Article 6, always considering good faith as guiding the application of the rule. Among them, the principles expressly listed of purpose; adequacy; need; free access; data quality; transparency; security; prevention; non-discrimination; and accountability.

---

[392] Art. 4º, II, LGPD.
[393] Art. 4º, III, LGPD.
[394] Art. 4º, IX, LGPD.
[395] Art. 5º, X, LGPD.
[396] Art. 2º.

As the previous chapter has already devoted to encompassing the general principles of data protection, this topic and its subtopics will only be left to make the correlation to the one already treated, presenting the peculiarities of the Brazilian model.

To this end, the principles brought in chapter 4 are illustrated in the central column, in green, from the document generated by Schwartz and Solove at The American Law Institute[397].

The side columns, in blue, represent the explicit principles of Article 6 of the General Data Protection Law. Its intersections will be explained, each of which, in its own topic.

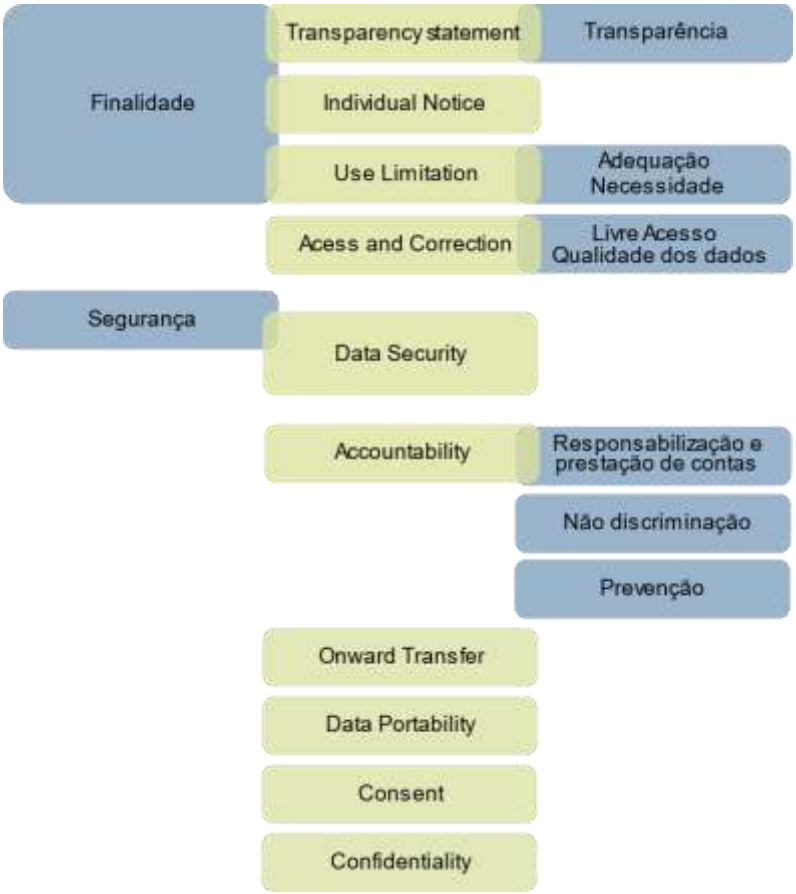


Figure 1. SOURCE: The Author

[397] From SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline.

5.2.1 Purpose

The principle of purpose, the first to be brought by the LGPD, is explained as the “processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes” (free translation)[398].

When the legal text says that the performance of the treatment has to be according to the purpose of it, this purpose necessarily needs to be legitimate. That is, coming from one of the legal bases, consent being one of them[399].

Thus, no data can be handled without its holder having prior knowledge, and, if necessary, the consent[400].

This prior knowledge can be achieved individually through the “individual notice”, or, more generally, and publicly by the “transparency statement”, making it clear that the database exists and why it exists. That is, its purpose.

While the “individual notice” or “transparency statement” determines that clear information should be given on how the data is processed to its holder or to the public, the "use limitation" limits the use of these not only to the consent, but to the “individual notice”.

Briefly, the purposes must be specific, explicit and informed to the holder, as well as in the "individual noticy" or by the "transparency statement". Just as further treatment is not permitted in a manner incompatible with these purposes, according to the "use limitation".

---

[398] Art. 6, I, LGPD.
[399] Other legal bases for legitimate treatment are contained in Art. 7, LGPD.
[400] Consent, as will be seen later, does not appear as a principle in isolation, but is implicit in different passages, as is the case with the purpose.

5.2.2 Adequacy

Adequacy, as the “compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing” (free translation)[401], represents the limitation of processing to “individual notice”.

"Use limitation", in it turns, limits the processing not only to “notice”, but also to the consent given.

Although the word "consent" is not expressly invoked to the compatibility of treatment in Brazilian norms, consent it is one of the legal bases for it, depending on the "context of processing".

As already emphasized, consent appears not as a principle, but as one of the legal bases of treatment, being therefore implicit in the lawfulness of the processing of any activity that depends on it.

5.2.3 Necessity

The principle of necessity deals with the

> limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing[402] (free translation);

It relates strictly to the former principle, also invoking the use limitation, but going beyond. For it is not enough that the holder has been notified about the use of his data. This use needs to be relevant, proportionate, and not excessive when compared to the purpose.

That is, it is classified more closely to the idea of minimization than of proper notification of the data subject and his eventual consent on the processing.

---

[401] Art. 6, II, LGPD.
[402] Art. 6, III, LGPD.

In this sense, the STJ[403] explicitly mentioned the principle of data minimization to declare abusive and illegal contractual clauses authorizing the bank to share consumer data with other financial entities, without the possibility of disagreeing with such sharing.

Thus, it is not concerned with seeking the notification or consent of the holder for the data to be collected, but it is interpreted whether this scope of treatment is necessary for the given purpose.

For example, the collection of personal data to open a registration. Name, age and email may be relevant data to achieve this purpose. Biometric records, facial recognition, or geolocation may not.

Thus, even if there is a prior consent on the collection of these latter data, the principle of necessity would prevent its treatment by extrapolating the purpose.

5.2.4 Free access and data quality

Free access as well as data quality is guaranteed by transnational principles through "access and correction", even though it is less comprehensive than those.

For the LGPD access must not only exist, but must be free and facilitated:

> IV - guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data[404] (free translation).

And correction should be guaranteed when the quality of the data does not correspond with the necessity or fulfillment of the purpose of its processing. Thus, clarity, accuracy and updating of this data are required:

> V – quality of data: guarantee to the data subjects of the accuracy, clarity,

---

[403] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1348532**. Relator: Ministro Luis Felipe Salomão, j. 10.10.2017.
[404] Art. 6º, LGPD.

> relevancy and updating of the data, in accordance with the need and for achieving the purpose of the processing[405] (free translation).

Article 18 of the LGPD details the right of the holder of the personal data to obtain from the controller, in relation to his/her data, by request:

> I – confirmation of the existence of the processing;
> II – access to the data;
> III – correction of incomplete, inaccurate or out-of-date data;
> IV – anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law;
> V – portability of the data to another service provider or product provider, by the means of an express request, pursuant with the regulations of the national authority, and subject to commercial and industrial secrets;
> VI – deletion of personal data processed with the consent of the data subject, except in the situations provided in Art. 16 of this Law;
> VII – information about public and private entities with which the controller has shared data;
> VIII – information about the possibility of denying consent and the consequences of such denial;
> IX – revocation of consent as provided in §5 of Art. 8 of this Law (free translation).

The law also concerned how this information will be provided to the data subject. In this sense, Article 19 indicates that confirmation of existence or access to personal data will be provided “I - immediately, in simplified form; or”; or “II - by means of a clear and complete statement indicating the origin of the data, the inexistence of registration, the criteria used and the purpose of the processing” (free translation), within 15 days of the requirement date.

However, free access does not mean unrestricted. There are several hypotheses in which there is the impossibility of meeting the claim, and in this case, one should at least communicate the reasons of fact or law that prevent immediate

---

[405] Art. 6º, LGPD.

action[406].

5.2.5 Transparency

Transparency is the “guarantee, to the data subjects, of clear, accurate and easily accessible information on the processing and the respective processing agents, subject to business and industrial secrets”[407] (free translation).

It couldn't be any different. The data subject, in in addition to having access to any of the other rights covered by the general principles, must have, primarily, extensive information on the processing of data. Only in this way can it be ensured that the legality, legitimacy, and security of treatment are ensured.

Without prejudice to confidentiality in specific cases, transparency is the basis that ensures ethical and respectful treatment of privacy and personality free development – premises of the LGPD.

The principle of transparency also underpins the Consumer Protection Code, which is applied to the many consumer relationships involving data processing. In this, clear and appropriate information to the consumer cannot be infringed[408].

In this sense, transparency is an essential point to ensure the rebalancing between the vulnerable of the relationship and the one who holds the information.

The principle of transparency could also be interpreted in accordance with the transnational principle of transparency statement, in the sense that, to comply it is necessary to have public knowledge of the database and that its performance is by the legal parameters.

In any case, the transnational principle relates more closely to the public

---

[406] Art. 18, § 4º, LGPD.
[407] Art. 6º, VI, LGPD.
[408] Art. 6º, III, art. 31 and art. 43, § 2º, CDC.

existence of the database. While the LGPD expands its application to all treatment processes, as a precondition for an ethical action.

5.2.6 Security

The LGPD treats security as the “use of technical and administrative measures able to protect the personal data from unauthorized accesses and from accidental or unlawful situations of destructions, loss, alteration, communication or diffusion”[409] (free translation). That is, in the context of "Data security", which in English terminology is distinguished from "data protection", as already delimited.

Such measures shall be used from the design of the product or service to the implementation of it[410], by all persons who intervene at any stage of processing, even after the end[411].

Similarly, systems must be structured to meet standards of good practice and governance and meet security requirements[412].

Protecting data security is also protecting all other rights already listed. This is because, when data is accessed, erased, lost or adulterated, the damage to the other rights of the holders is permanent.

In addition to exposing data subjects to privacy, events like this also discredit the controller's reputation and cause a sense of social insecurity about confidence in giving up data.

Therefore, the lack of security is provided for as irregular treatment subject to possible administrative sanctions, which will be explained in its topic.

---

[409] Art. 6º, VII, LGPD.
[410] Art. 46, § 2º, LGPD.
[411] Art. 47, LGPD.
[412] Art. 49, LGPD.

5.2.7 Liability and accounting

The liability and accounting, as principles, demand the "proof, by the agent, of adoption of effective measures able to prove observance of and compliance with the personal data protection rules, and also with the effectiveness of these measures"[413].

Thus, it alerts the controllers and operators that they are responsible for complying with the legal requirements of the LGPD.

> And it is not enough just to want to comply with the Law, it is necessary that the measures adopted for this purpose are proven effective. That is, agents should, throughout the data processing life cycle under their responsibility, review legal compliance and implement personal data protection procedures in accordance with their own risk weighting[414] (free translation).

Regarding accountability, the law provides that the controller keeps track of the processing of personal data that it performs, so that the regulatory authority (ANPD) can request this information at any time[415]. These same records must be available for possible defense in court proceedings, in particular to reverse the burden of proof in favor of the data holder, when legal requirements are present, which are: the likelihood of the claim, hypossuficence of producing evidence or when this production is excessively burdensome to the holder[416].

The law left no doubt about the liability of both the controller and the operator, due to the exercise of the activity of processing personal data: when it causes harm to others, whether in the patrimonial, moral, individual or collective sphere, the obligation to repair will be born[417].

Exceptions to liability are restricted to three hypotheses: (i) that there was no processing in question, (ii) that although there was data processing, there was no

---

[413] Art. 6º, X, LGPD.
[414] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.).**LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 166-167.
[415] Art. 55-J, IV, LGPD.
[416] Art. 42, § 2º, LGPD.
[417] Art. 42, caput, LGPD.

violation of the LGPD or, (iii) that the damage caused is due the data subject or third party sole fault[418].

It is then up to the controller to analyze, under his responsibility, the application of the standard; the legal basis for processing to justify legitimate interest; where the legal basis is consent, that it is given freely, unequivocally and informed; if the requirements of transparency, security, among all others already mentioned are present.

5.2.8 Non-Discrimination, Prevention, Portability, Confidentiality, Consent and Onward Transfer

The principle of non-discrimination, listed by the LGPD as a "impossibility of processing data for discriminatory, unlawful or abusive purposes"[419] (free translation).

Although not within transnational principles, avoiding discriminatory, unlawful, or abusive purposes are presupposition of all State legal systems. It is through systematized reading among other norms that this treatment will be considered discriminatory.

Prevention, to the same extent, as the "adoption of measures to prevent the occurrence of damage in view of the processing of personal data"[420] (free translation), it is related to the mitigation of liability, as well as to acting prudently to ensure the realization of the other principles.

It is included to modify the culture in data processing to reduce risks whenever possible, or at least reduce the impact of damage.

On the other hand, the transnational principles brought in Chapter 4 cover

---

[418] Art. 43, I-III, LGPD.
[419] Art. 6º, IX, LGPD
[420] Art. 6º, VIII, LGPD.

Onward Transfer, Data Portability, Confidentiality, and Consent. And these, although they do not correspond directly to a "principle", as listed in Article 6 of, also appear in the Brazilian General Data Protection Law, in different provisions.

Data portability, even if it does not appear as a normative principle, is specified as the Data Subject's Right, as follows:

Data portability, even if it does not appear as a normative principle, is specified as the Data Subject's Right, as follows:

> Art. 18. The data subjects are entitled to obtain from the controller, in relation to the data of the data subjects processed by such controller, at any time and upon request: (...) V- portability of the data to other service providers or suppliers of product, at the express request, and observing the business and industrial secrets, in accordance with the regulation of the controlling body[421] (free translation).

That is, the right of the data subject to obtain from the controller, in a structured way, his personal data is protected, so that he can transmitted to another controller.

The idea of portability is not to technologically imprison the user to a permanent bond with the controller, whose exchange would bring him excessively high costs and capable of demotivating the replacement. Thus, it is closely linked to freedom of choice[422].

Issues such as technical measures and permissible formats for compliance should still be regulated.

As for confidentiality, it appears in relation to the safeguarding of trade and industrial secrecy that must be observed and preserved in the face of the principle of transparency.

Consent, on the other hand, is not listed as a principle in the LGPD, but it

---

[421] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais** (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018.
[422] BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019, p. 231.

is considered a normative guideline to determine whether the processing of personal data is fair and lawful[423].

The word "consent" appears thirty-seven times in law and as the first legal basis hypothesis for the processing of data[424]. Thus, although nine other legal bases are authorizing the processing of[425], consent is especially relevant when it comes to children's data.

Article 14, in its Paragraph 1, restricted the processing of children's personal data to the legal basis of "specific and prominent" consent, given by at least one parent or legal guardian.

The exception is only in the possibility of data collection “whenever the collection is necessary to contact the parents or the legal guardian, used a single time and without storage, or for their protection, (…)”[426] (free translation).

The same paragraph continues its text to bring the contours of Onward Transfer**,** since it determines that “they cannot be transferred to third parties, under any circumstance, without the consent set forth in paragraph 1 of this article” [427] (free translation).

The same rule appears in other articles of the LGPD with the sealing of data sharing with third parties, without being guided by any of the legal bases.

---

[423] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 175-176.
[424] Art. 7º, inc. I, LGPD.
[425] Article 7 The personal data can only be processed in the following events: I – by means of the data subject's consent; II – for compliance with a statutory or regulatory obligation by the controller; III - by the public administration, for the processing and shared use of data required for the performance of public policies set forth in laws or regulations or supported by contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law; IV – for the conduction of studies by research bodies, guaranteeing, whenever possible, the anonymization of personal data; V – whenever necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject; VI – for the regular exercise of rights in lawsuits, administrative or arbitration proceedings, the latter pursuant to the provisions of Law No. 9.307, of September 23, 1996 (Arbitration Law); VII – for protection of the life or of the physical safety of the data subject or of third parties; VIII – for protection of the health, in a procedure carried out by health professionals or by sanitary entities; IX – whenever necessary to serve the legitimate interests of the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject, which require protection of the personal data; or X – for the protection of credit, including with respect to the provisions of the applicable law. (free translation).
[426] Art. 14, § 3º, LGPD.
[427] Art. 14, § 3º, LGPD.

However, the protection of children's data protection in Brazil is not restricted to the General Data Protection Law and should be interpreted from the dialogue with the other sources – at least internal – of the law, as will be seen below.

5.3 The protection of children's data from dialogue with other internal sources

Because it is the central object of analysis of the thesis, the General Data Protection Law will be analyzed and interpreted here from the dialogue of the sources of the Brazilian legal system.

This term, "dialogue of the sources", was coined by Erik Jayme "signifying the current simultaneous, coherent and coordinated application of the legislative sources, special laws (...) and general (...), with convergent but not equal fields of application"[428] (free translation).

The term dialogue refers to reciprocal influences and joint application of more than one standard at the same time and in the same case. When dealing with children's data protection, it could not be different.

On the one hand, there is the Special Data Protection Law (LGPD) and on the other hand, the special law for the protection of children and adolescents (Statute of children and adolescents – ECA). It is still to be considered when there is a consumer relationship, and therefore the application of the Consumer Protection Code (CDC). And, of course, all interpretation necessarily needs to be given in the light of the Federal Constitution.

There is no need to speak, however, of conflict of laws, a common expression in intertemporal law. In conflicts there is the interposition with prevalence of one law over the other and the consequent exclusion of the other from the system

---

[428] MARQUES, Claudia Lima. Diálogo das Fontes in BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual do Direito do Consumidor.** 5 ed. Ver., atual. E ampl. São Paulo: Editora Revista dos Tribunais: 2013, p. 122.

(by abrogate, derogation or revocation)[429].

On the contrary, what the dialogue of the sources seeks is harmony between them, framing the legal system as an integrative system. This flexible system allows the coexistence of norms in search of achieving their declared purpose.

For analysis of the child's data protection, it is necessary to consider, then: the General Data Protection Act with the purpose of “protecting the essential rights of freedom and privacy and the free development of the personality of the individuals”[430] (free translation); the Statute of the Child and Adolescent, which provides for "full protection of children and adolescents”[431], guaranteeing them all fundamental rights and ensuring “every opportunity and facilities in order to provide them with physical, mental, moral, spiritual and social development, in conditions of freedom and dignity”[432]; also, because it is often the relationships of consumption, the Consumer Protection Code that has the "recognition of consumer vulnerability in the consumer market”[433].

5.3.1 Hypervulnerability

The Consumer Protection Code is based on the principle of consumer vulnerability, with constitutional recognition (Art. 5, XXXII, and Art. 170, V), and on the Code itself, as one of the objectives of the National Consumer Relations Policy (Art. 4, I).

The notion of vulnerability is associated with

> the identification of weakness or debility of one of the subjects of the legal relationship on the basis of certain conditions or qualities inherent to it or, furthermore, a position of strength which can be identified in the other

---

[429] MARQUES, Claudia Lima. Diálogo das Fontes in BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual do Direito do Consumidor.** 5 ed. Ver., atual. E ampl. São Paulo: Editora Revista dos Tribunais: 2013, p. 123.
[430] Art. 1º, LGPD.
[431] Art. 1º, ECA.
[432] Art. 3º, ECA
[433] Art. 4º, I, CDC.

> subject of the legal relationship[434] (free translation).

The principle aims to ensure formal-material equality to the subjects, rebalancing the legal relationship of consumption. Vulnerability, in this sense, is presumed for the entire category of consumers. Thus, every consumer is vulnerable. There's no exception.

However, the doctrine improved the classification of the vulnerable, while creating the classification of "hypervulnerable"[435]. Hypervulnerability is characterized by an objective situation of worsening the vulnerability of the consumer individual:

> [...] would be the phatic and objective situation of aggravation of the vulnerability of the consumer natural person, by apparent or known personal circumstances of the supplier, such as his reduced age (so the case of baby food or advertising for children) or advanced age (thus, special care for the elderly, both in the Code in dialogue with the Statute of the Elderly and credit advertising for the elderly) or a healthy situation (as well as gluten allergy and information in the medicine leaflet)[436] (free translation).

Therefore, when classified in this category, it is admitted that the hypervulnerable group needs greater protection, and the interpretation of the norm should be concerned with this rebalancing brought by the constitutional principle.

In the same way, the Federal Constitution of 1988 considers "vulnerable" and establishes special protection for consumers (art. 48) and for the protection of children and adolescents (chapter VII).

That is, the child consumer appears twice in the vulnerability list, and, according to the classification pointed out, falls into this category of hypervulnerability.

Therefore, the first item to dialogue with the protection of children's data is its classification of hypervulnerable, especially when related to advertising aimed at them, as a consumer.

The LGPD, by implementing the protection of fundamental rights as an

---

[434] MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2014, p. 164.
[435] MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2014, p. 184.
[436] MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2014, p. 201-202.

objective of the law[437], exposed the vulnerability of the data subject in relation to the data processing agent. Only one side is granted protection for considering it uneven of forces.

This idea of vulnerability approaches the type of protection given to consumers by the Consumer Protection Code, which derives from the understanding of the social function of private law to protect the citizen from the challenges of a massified, globalized, computerized society, which ultimately reflects on its fundamental right to human dignity[438].

5.3.2 Comprehensive children protection

The Federal Constitution of 1988, in its art. 227 and the 'Statute of the Child and Adolescent' confer comprehensive, special and priority protection to natural people in developing condition: children and adolescents.[439]

> Comprehensive protection should be understood as the set of rights that are proper only to immature citizens; these rights, unlike those fundamental ones recognized to all citizens, are in pretensions not so much in relation to negative behavior (refraining from the violation of those rights) but as positive behavior by the public authority and other citizens, as a rule of interest in ensuring this special protection. In force of comprehensive protection, children and adolescents have the right for adults to do things for them[440].

The principle of comprehensive protection guides the construction of the entire legal system to protect the rights of children and adolescents. It assumes that these persons cannot exercise their rights on their own and therefore need third parties (family, society, and state) to protect their fundamental legal assets.

---

[437] Art. 1º, second part, LGPD.
[438] BENJAMIN, Antônio Herman Vasconcellos; BESSA, Leonardo Roscoe; MARQUES, Cláudia Lima. **Manual de direito do consumidor**. 5. ed., ver., atual. e ampl. São Paulo: Revista dos Tribunais, 2013, p. 47.
[439] In it, the constituent established as the duty of the family, society and the State to ensure the child, adolescent and young, with absolute priority, the right to life, health, food, education, leisure, professionalization, culture, dignity, respect, freedom and family and community coexistence, in addition to putting them safe from all forms of neglect, discrimination, exploitation, violence, cruelty and oppression.
[440] CURY, Munir (coord.). **Estatuto da criança e do adolescente comentado**: comentários jurídicos e sociais. 9ª ed., atual. São Paulo: Malheiros, 2008, p. 36

Thus, to say that children are in a position of vulnerability, or hypervulnerability in relation to their personal data – dialoguing with the Consumer Protection Code, means admitting that they will not have the same discernment and control over their data as an adult, and, for all the reasons already exposed, need special protection.

In this particular point, it should be noted that Brazil is a signatory to the Convention on the Rights of the Child[441], in force since 1990, which confers on this population, worldwide, for the first time, all rights so far reserved for adults, including those registered in the Universal Declaration of Human Rights of 1948.

The document also states that these rights must be exercised without any discrimination of race, color, sex, origin, religion, economic position or physical disability; and that all actions relating to the child should consider primarily their best interests.

In Brazil, there was a great impact on how to understand and protect childhood from the end of the 1980s, with the promulgation of the Constitution, the establishment of public policies for childhood and adolescence and the signing of international treaties such as the Convention.

The indicators[442] show that these impacts could be felt in several areas: the average illiteracy rate among children and adolescents aged 10 to 18 years fell by 88.8%; school dropout, of adolescents aged 15 to 17 years, fell by almost 50%; between 1990 and 2012, the infant mortality rate of children up to 1 year of age fell by 75%; from 1992 to 2013, the number of children aged 5 to 15 in child labor fell by 76%; and, from 1994 to 2014, the total number of undernourished persons fell by 84.7%.

However, in 2016, infant mortality in the country, after 26 years in the fall,

---

441 UNICEF. **Convenção sobre os Direitos da Criança**. Brasília: UNICEF, 1989. Available at: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Accessed 09 May, 2022.

442 PRIORIDADE ABSOLUTA. **Panorama**: dados sobre a infância e adolescência brasileiras. Available at: <https://prioridadeabsoluta.org.br/estatuto-crianca-adolescente/panorama-infancia-adolescencia/> Accessed 09 May, 2022.

went back up; on average, two children up to 5 years old still die per day in Brazil due to diarrhea, which could be avoided with access to drinking water, hygiene measures and basic sanitation.

Issues related to social inequality, access to quality education and violence are also latent among children in Brazil.

That is, despite reaching important milestones, the protection of the child, in an integral way, as proposed by the Federal Constitution and the Statute of the Child and Adolescent still lacks long work to achieve the expected effectiveness.

For this reason, in the last chapter, some of the rights listed by the legislation for childhood protection will be brought, based on the prioritization of the best interest, applied to the protection of their data.

5.3.3 Protection against misleading and abusive advertising, coercive or unfair commercial methods, and abusive practices or terms

The Consumer Protection Code disciplined, in its art. 43, the databases of consumers. It provides that consumers must be notified of the opening of a personal database unsolicited by him[443]. In addition, the database operator will have the duties of: ensuring access by the consumer[444]; accuracy of the information; that the database be restricted for clear and true purposes and, finally; that the five-year time limit for the storage of negative information be observed[445].

The consumer may also demand the immediate correction-cancellation of incorrect information or that has exceeded the time limit[446].

Finally, the interpretation given to the provisions of the Consumer Protection Code must be based on its principled basis of transparency and good

---

[443] Art. 43, § 2, CDC.
[444] Art. 43, caput, CDC.
[445] Art. 43, § 1, CDC.
[446] Art. 43, § 3º, CDC.

faith[447].

5.4 Child data protection in LGPD

From the dialogue of the sources, proposed in the previous topic, will now be analyzed the articles of the LGPD that deals specifically with the protection of children's data.

Although the LGPD did put the personal data of children and adolescents in the list of sensitive data of Art. 5, II, the law prints stricter obligations for its processing. In other words, the processing of personal data of children and adolescents requires more cautious measures for their protection.

The LGPD has organized in a synthetic, and perhaps even simple way, the protection of children (and adolescents) in relation to personal data, in section III, called “The Processing of Personal Data of Children and Adolescents”, which has only one article (art. 14) and six paragraphs.

It starts by saying that the “the processing of personal data of children and adolescents shall be carried out to their best interest, pursuant to the provisions of this article and of the applicable law”[448].

The best interest highlighted in Article 14 comes from the Convention on the Rights of the Child[449], which defines that: “

> Article 3.1 In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.

That is, it is not in the interest of parents or legal representatives to receive priority attention to the processing of children's data. Nor even the interest of third

---

[447] Art. 4º, CDC.
[448] Art. 14, LGPD.
[449] UNICEF. **Convenção sobre os Direitos da Criança**. Brasília: UNICEF, 1989. Available at: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Accessed 09 May, 2022.

parties.

In slight, the principle of the best interest of the child excels in an absolute way so that they are guaranteed their fundamental rights expressed in the Federal Constitution of 1988[450], in the Statute of the Child and Adolescent[451], and other protective rules, such as the LGPD, including, then on the roll, the right to data protection.

The article continues in its first paragraph, at the disposal that: “the processing of personal data of children shall be carried out with the specific and separate consent of at least one of the parents or by the legal guardian” (free translation).

As already pointed out, consent is the only legal basis for the processing of children's data that appears, expressly, in the article. The only exception proposed in the following paragraph:

> Paragraph 2º In the processing of data set forth in paragraph 1 of this article, the controllers shall maintain public the information on the types of data collected, the form of use thereof and the procedures for exercise of the rights referred to in article 18 of this Law (free translation).

Two points deserve special attention in this regard. The first, the fragility of consent as a legal basis. And the second, the need to use the data to preserve the best interest of the minor without the consent of the parents.

Regarding the first, the whole question related to the possibility of fraud, even by the child, in the realization of consent, the lack of understanding of the scope of what is consented, among other factors that, in general terms, has already been explored in previous topics; will be especially highlighted in the last chapter regarding the need to re-evaluate the theory of consent.

The second point is the need for an extensive interpretation, in dialogue with the other sources of law, to understand that it will not always be necessary the

---

[450] Art. 227, CF.
[451] Art. 4º, ECA.

consent of those responsible for the processing of children's data. For example, when there is a regulatory legal duty to process data, the "best interest" referred to in the caput may be classified, in the exception of the "protection" of the minor brought in Paragraph 3.:

> Paragraph 3º Personal data of children may be collected without the consent referred to in paragraph 1 of this article whenever the collection is necessary to contact the parents or the legal guardian, used a single time and without storage, or for their protection, and they cannot be transferred to third parties, under any circumstance, without the consent set forth in paragraph 1 of this article.

Of course, for treatments for commercial purposes, there is no need to speak of "best interest" overriding consent. In this case, the interpretation of the best interest is given from the consent of the parents or guardians.

Another important highlight given by the LGPD to child protection is the non-conditioning of the provision of data for participation in games, applications or other activities, in addition to those strictly necessary for the activity[452].

The definition of what would be necessary for the activity should be interpreted restrictively when the public is childish, from the principle of necessity.

Another criterion brought by the LGPD, in art 14, paragraph 5, was about verification of consent, giving the controller the obligation to perform “all reasonable efforts to confirm that the consent to which paragraph 1 of this article refers was given by the person responsible for the child, considering the available technologies.”. Something similar to what was brought by COPPA, as seen in the specific item (6.2.1), however, U.S. law regulated specific verification methods to achieve this purpose.

In Brazil, there is still no clear definition of what reasonable efforts or ways to guarantee it would be. It will be left to the regulation, doctrine or courts the role of interpreting the standard broadly or on a case-by-case basis.

---

[452] Art. 14 (...) § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Finally, Article 14 concludes with paragraph 6, highlighting that all information on the processing of children's data must be provided in a “clear, simple and accessible manner, considering the physical and motor, perceptive, sensorial, intelectual and mental characteristics of the users”, that is, different for each age group, and even “with the use of audiovisual resources whenever appropriate, in order to provide the necessary information to the parents or to the legal guardian, as appropriate for the children’s understanding”.

Again, the way this will be done still lacks explanations, which are expected to be given by the Regulatory Authority. What do these features mean? Should drawing language be used? How to ensure accountability in these cases?

It is not strictly about how consent is asked, but it is also linked to the transparency statement, and the individual notice, which should also be based on these criteria.

However, the importance since paragraph for the thesis is in the first part, in which it considers different approaches to depend on the physical-motor characteristics, perspectives, sensory, intellectual, and mental characteristics of the user.

Therefore, different strategies are required depending on the age at which the content is being targeted. Something that has been completely ignored so far by data protection laws, which approach the child as a single group with linear characteristics.

On the contrary, as it was brought in chapter 3 and will also be addressed in the last chapter, to preserve that intellectual freedom, dignity, privacy, among many other inherent rights, It is necessary to consider the peculiarities of human development in each phase.

Certainly, the ability of a 2-year-old to consent in place of the parents will not be the same as one of 11. As well as the interest of a 10-year-old child to access certain content would be irrelevant to a 3 and so on.

Therefore, it is important to consider the multiplicity of characteristics tied to the children's group when proposing regulations on the subject or interpreting the application for their best interest.

5.4.1 National Data Protection Authority

The National Data Protection Authority (ANPD) was sanctioned in 2018 and sanctioned in 2019 with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person, guided by the provisions of the LGPD. Thus, it is responsible for ensuring, implementing, and supervising compliance with the law[453].

Initially as a body linked to the Presidency of the Republic, therefore part of the Executive Power of the Federal Government, endorsed only with technical and decision-making autonomy, it became a National Authority, of a special nature, in June 2022 through Provisional Measure No. 1,124[454].

Thus, it began to have its own assets and administrative and budgetary autonomy, maintaining the structure and competencies already existing.

The attributions, provided in the LGPD, in Article 55-J, are, among others: ensuring data protection and compliance with trade and industrial secrets; to monitor and apply sanctions, through administrative proceedings; to assess petitions; promote knowledge of public standards and policies and security measures; promote and develop studies on national and international practices; encourage the adoption of standards for services and products that facilitate the exercise of control of holders over their personal data; promote cooperation actions with authorities for the protection of personal data from other countries, of an international or transnational nature; conduct audits, or determine their conduct.

---

[453]FEDERAL SENATE. **Provisional measure No. 869** of 27 December 2018. Amends Law No. 13,709 of August 14, 2018, to provide for the protection of personal data and to create the National Data Protection Authority and provides other measures. Available at: <https://legis.senado.leg.br/norma/30762959/publicacao/30762970> Accessed 28 Jun., 2022.

[454] However, for the Provisional Measure to be definitively transformed into law, it will still depend on the approval of the House of Representatives and the Federal Senate.

In addition, it also includes c to issue a commitment to treatment agents to eliminate irregularity, legal uncertainty or litigation situation in administrative proceedings; edit standards, guidelines and procedures; deliberate, in the administrative sphere, on a final, on the interpretation of the Law, its powers and the cases omitted; liaise with public regulatory authorities to exercise their competences in specific sectors of economic and governmental activities subject to regulation; implement simplified mechanisms, including electronic means, for the registration of complaints about the processing of personal data in non-compliance with the Law[455].

That is, the ANPD, the authority to prepare the guidelines that regulate the processing of personal data and to monitor and apply penalties in case of non-compliance with the law, also has the function of informing and making the population aware of data protection policies, practices and data rights, as well as stimulating the understanding of standards by companies that make use of personal data and information.

In this sense, it approaches the attributions of the Federal Trade Commission (FTC), which will be addressed in the next chapter, as the U.S. regulatory agency. However, the FTC does not act only in the data protection area, unlike the Brazilian one that was created exclusively with this competence.

5.4.2 Administrative sanctions

Unlike the wording brought in the Civil Framework of the Internet, which confers the competence of administrative sanctions to the "competent body", the LGPD brought, in Article 52, when inaugurating Section I of Chapter VIII – Of the Supervision, the unambiguous legal provision of the exclusive competence of the National Authority.

This differentiation brought hermeneutic delimitation around the exercise of supervisory power. Thus, it is avoided that the Judiciary is given the power to apply administrative penalties, as happens to substantiate much of the judicial decrees to

---

[455] Items I to the XXIV.

block internet applications, based on the open interpretation of the Civil Framework of the Internet[456].

Sanctions are provided in Article 52 of LGPD:

> I – warning, with indication of a term for adoption of corrective measures;
>
> II – simple fine of up to two percent (2%) of the sales revenue of the legal entity of private law, group or conglomerate in Brazil in its last fiscal year, excluding taxes, limited, in the aggregate, to fifty million Reais (R$50,000,000.00) per infraction;
>
> III – daily fine, with due regard for the total limit referred to in item II;
>
> IV – disclosure of the infraction after it has been duly investigated and its occurrence has been confirmed;
>
> V – blockage of the personal data to which the infraction relates, until regularization thereof;
>
> VI – elimination of the personal data to which the infraction relates;
>
> VII – partial or total suspension of the operation of the database to which the infraction relates for a maximum period of six (6) months, which can be extended for an identical term until regularization of the processing activity by the controller;
>
> VIII – suspension of performance of the personal data processing activity to which the infraction relates, for a maximum term of six (6) months, which can be extended for an identical term;
>
> IX – partial or total prohibition of the performance of any activities relating to data processing (free translation).

The legal text also provides that the sanctions will be applied after administrative procedure that allows the broad defense and according to the peculiarities of the specific case[457].

Among the criteria for the evaluation of penalties, are conditions relevant to the offender such as: good faith; the advantage granted or intended; the economic condition; recidivism; cooperation; the repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage, aimed at

---

[456] ALVES, Fabricio da Mota. Chapter VIII: surveillance in BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD**: General Data Protection Law Commented. Sao Paulo: Thomson Reuters Brazil, 2019, p. 268-369.
[457] Art. 52, § 1º, LGPD.

the safe and adequate treatment of data; the adoption of a policy of good practice and governance; and the prompt adoption of corrective measures[458].

As well as criteria relating to the damage: the severity and nature of the offences and personal rights affected; the degree of damage; proportionality between the severity of the fault and the intensity of the sanction[459].

Thus, chapter 5 concludes, which aimed to understand the protection of children's data in the Brazilian legal system, from a reading dialogued with other legal sources beyond the General Data Protection Law. In the next chapter, the same topics will be addressed, however, from the American legal system point of view.

[458] Art. 52, § 1º, LGPD.
[459] Art. 52, § 1º, LGPD.

CHAPTER 6
PROTECTION OF CHILDREN'S DATA IN THE UNITED STATES

This chapter will focus on the peculiarities of the Children's Privacy Protection Act (COPPA)[460], a U.S. federal law that provides data protection for children under the age of 13.

For analysis of the law will be considered recent articles published in the U.S. legal-academic journals, made available by the agreement with Widener University (Delaware Law School).

The topics were selected to confront the same elements in the Brazilian norm and cover the main points of convergence and divergences between them.

6.1 COPPA comprehensiveness

6.1.1 Who is protected

In the United States, there is no legal standard for the concept of "child", with each law being left to define age within the scope of its application. A child is considered, for example, under 21 years of age for Criteria of U.S. citizenship[461].

In most states, it is considered child the under 18, however, for the state of Alabama and Nebraska refers to the age of 19 and for Mississippi, 21 years old[462].

In recommending the creation of a specific child data protection law, the Federal Trade Commission, through the 1998 report, explored different levels of

---

[460] 15 U.S.C. §§ 6501-6506 (2018). **Children's Online Privacy Protection Act of 1998**. Available at: <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim#sourcecredit> Accessed 12 Jul., 2021.

[461] UNITED STATES. **Child Status Protection Act.** PUBLIC LAW 107–208—AUG. 6, 2002 116 STAT. 927. Available at: <https://www.congress.gov/107/plaws/publ208/PLAW-107publ208.pdf> Accessed 07 Jul., 2021.

[462] STATE LEGAL AGES LAWS. Available at: <https://statelaws.findlaw.com/family-laws/legal-ages.html> Accessed 09 Jul., 2021.

protection for different ages.

> Children's privacy legislation also would recognize that a marketer's responsibilities vary with the age of the child from whom personal information is sought. In a commercial context, Congress and industry self-regulatory bodies traditionally have distinguished between children aged 12 and under, who are particularly vulnerable to overreaching by marketers, and children over the age of 12, for whom strong, but more flexible protections may be appropriate[463].

Thus, the initial suggestion was to provide notification and obtain parental consent for websites that collected data from children up to 12 years of age.

In other years, for those over 13 years of age, there would be no need for consent, but still, there would be an obligation to provide notice to parents about the collection of such information, while also giving them the opportunity to remove them from the site database (opt-out).

The bill that took place next year, authored by Senators Bryan and McCain, also made mention to "provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of twelve and under the age of 17"[464].

However, the possibility of parents having prior access and some kind of control over the navigation of adolescents caused companies and civil liberties groups to manifest themselves in opposition[465]. This is because, "requiring teens to obtain parental permission might curtail their ability to access information about birth control and abortion, or resources for getting help in abusive situations"[466].

---

[463] LANDESBERG, Martha K., LEVIN, Toby Milgrom; CURTIN, Caroline G.; LEV, Ori., **Federal Trade Commission, Privacy Online**: a report to congress (1998), p. 42. Available at: <https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf> Accessed 10 Ago., 2021.

[464] U.S. GOVERNMENT PRINTING OFFICE. **Children's Online Privacy Protection Act of 1998**, S. 2326, 105th Cong. §3(a) (1998). Available at: <https://www.congress.gov/bill/105th-congress/senate-bill/2326/text> Accessed 10 Ago., 2021.

[465] JARGAN, Julie. How 13 Became the Internet's Age of Adulthood: The inside story of COPPA, a law from the early days of e-commerce that is shaping a generation and creating a parental minefield. **The wall street journal**. June 18, 2019. Available at: <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> Accessed 10 Ago., 2021.

[466] JARGAN, Julie. How 13 Became the Internet's Age of Adulthood: The inside story of COPPA, a law from the early days of e-commerce that is shaping a generation and creating a parental minefield. **The wall street journal**. June 18, 2019. Available at: <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> Accessed 10 Ago., 2021.

Thus, given the interest aligned between companies and civil liberties groups, there was no alternative but to succumb to the age restriction.

In enacting the law, it was then confirmed that *the Children's Privacy Protection Act* (COPPA) protects children up to 13 years of age without any variability of age restrictions.

The reflections of the decision are clear in the privacy policy of most websites and applications, which only came into existence after this period since the law came into force seven years before the creation of the first commercial smartphone (Apple's Iphone).

Thus, instead of seeking parental consent, social media applications and platforms eventually formally deny access to children under the age of 13, as a way to divert the need for COPPA compliance.

However, the reality is that children use these resources, lying age, often with the consent of their own parents, but staying on the margins of regulation. Similar situation will be discussed in the case "YouTube", addressed in its own title.

COPPA did not limit, however, that states can provide stricter requirements by state law, including with greater age coverage.

The Act is applied to anyone who operates a website located on the Internet or an online service and who collects or maintains personal data from or about users and visitors, or on behalf of whom such information is collected or maintained; in any U.S. territory, or who is a party to an international transaction[467].

---

[467]§6501. Definitions In this chapter: (1) Child The term "child" means an individual under the age of 13. (2) Operator The term "operator"- (A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce- (i) among the several States or with 1 or more foreign nations; (ii) in any territory of the United States or in the District of Columbia, or between any such territory and- (I) another such territory; or (II) any State or foreign nation; or (iii) between the District of Columbia and any State, territory, or foreign nation; but (B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 45 of this title. UNITED STATES. Pub. L. 105–277, div. C, title XIII, §1301, Oct. 21, 1998, 112 Stat. 2681–728, provided that: "This title [enacting this chapter] may be cited as the **'Children's Online Privacy Protection Act of 1998'**". Available at:

It includes, therefore, who owns and/or controls the information, who pays for its collection and maintenance, who actually participates in the collection or is only a data transmission channel between different entities[468].

Internet access providers, which do not collect or provide children's content, are not covered by the standard. As well as non-profit entities are excluded for not being covered under the Federal Trade Commission Act.[469]

6.1.2 Which data is contemplated

COPPA applies to "personal information" of children collected by operators of websites and digital services for commercial purposes, including *mobile apps and Internet of Things* (IoT) devices, that have content targeted at children.

The Act covers websites and applications that are not directed to children, but that have real knowledge that they collect, use, or pass on personal information of children under 13 years, even as third parties[470].

The meaning of "having real knowledge" was asked to the regulatory agency. In response, it was stipulated that there is no need for operators of sites with general public, that is, those that are not specifically intended for children, to investigate the age of their visitors. However, when collecting information that identifies this child as such, either through a direct question of age, schooling or similar, the websites and applications needs to comply with COPPA rules[471].

<http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim> Accessed 10 Aug., 2021.

[468] FEDERAL TRADE COMMISSION. 16th CFR Part 312. **Children's Online Privacy Protection Rule**: final rule. 59888 Federal Register / Vol. 64, No. 212 /Wednesday, November 3, 1999 /Rules and Regulations. Footnote 52. Available at: <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf> Accessed 28 Jun., 2021.

[469] FEDERAL TRADE COMMISSION. 16th CFR Part 312. **Children's Online Privacy Protection Rule**: final rule. 59888 Federal Register / Vol. 64, No. 212 /Wednesday, November 3, 1999 /Rules and Regulations. Footnote 213. Available at: <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf> Accessed 28 Jun., 2021.

[470] 15 U.S.C. §6501. (4)(b).

[471] FEDERAL TRADE COMMISSION. 16th CFR Part 312. **Children's Online Privacy Protection**

COPPA does not apply to information from children collected from parents or other adults[472]. Unlike Brazilian legislation, which cares about children's data, regardless of how they were collected, COPPA does not apply to information collected about children, only from children.

The exception is in the information obtained from parents in the course of obtaining parental consent. Nevertheless "the Commission expects that operators will keep confidential any information obtained from parents in the course of obtaining parental consent or providing for parental review of information collected from a child"[473].

As personal information, are:

> (A) a first and last name;
>
> (B) a home or other physical address including street name and name of a city or town;
>
> (C) an e-mail address;
>
> (D) a telephone number;
>
> (E) a Social Security number;
>
> (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
>
> (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph[474].

The protection of Brazilian legislation, in this sense, is broader than the North American legislation, when considering all data collected from individuals for commercial purposes, in addition to ensuring the protection of children's data,

---

Rule: final rule. 59888 Federal Register / Vol. 64, No. 212 /Wednesday, November 3, 1999 / Rules and Regulations, p. 6. Available at: <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf> Accessed 28 Jun., 2021.

[472] 15 U.S.C. § 6501(b); 16 C.F.R. §312.3.

[473] FEDERAL TRADE COMMISSION. 16th CFR Part 312. **Children's Online Privacy Protection Rule**: final rule. 59888 Federal Register / Vol. 64, No. 212 /Wednesday, November 3, 1999 /Rules and Regulations, p. 6. Available at: <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf> Accessed 28 Jun., 2021.

[474] 15 U.S.C. § 6501 (8).

regardless of the source of obtaining being an adult.

6.2 Legal fundamentals or regulatory framework

6.2.1 Consent

The parental consent requirement is an important aspect of the COPPA that places parents in control of their child's online communications.

Under COPPA, expect in certain limited cases, under 13 kids' personal information may not be collected or used without explicit and verifiable consent from a parent.

It is noteworthy that the model established by COPPA is opt-in, that is, it takes a positive action to collect the data, being, in this case, executed by parents or guardians[475].

In this way, all COPPA regulations revolve around consent. There is no restriction on children's access to certain websites, for example, this access filter is the responsibility of parents or legal guardians. If consent is required, the company complies with COPPA.

Thus, the law requires companies to make a reasonable effort to ensure that they have received the consent of a parent and not from a child. Methods of obtaining consent include talking to a parent by phone or video chat, obtaining credit card information or communicating through multiple emails[476].

With consent, companies may collect personal information from children as long as they do not require more information than is necessary for a child to

---

[475] § 312.5 Parental consent. An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.
[476] 15 U.S.C. §6501(9); 16 C.F.R. §312.3; 312.5.

participate.

This latter prohibition is important and is consistent with the principle of data minimization and use limitation, as explored in the chapter itself. However, to date, there is no specific regulation on the data collected – with consent, which leads to the conclusion of the rule's lack of execution in this sense.

On the contrary, the regulatory agency's recent demonstrations regarding COPPA's failure to comply with the failure to obtain consent. That is, the demands are not given by data consented and, later, used improperly (see topic Penalties of this item).

The COPPA Rule says that an operator must choose a method reasonably designed in light of available technology to ensure that the person giving the consent is the child's parent.

Neither COPPA nor LGPD mandate the method a company must use to get parental consent. The FTC, however, has determined that a few consent methods meet that standard[477]:

> a) sign a consent form and send it back to you via fax, mail, or electronic scan;
>
> b) use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
>
> c) call a toll-free number staffed by trained personnel;
>
> d) connect to trained personnel via a video conference;
>
> e) provide a copy of a form of government-issued ID that you check against a database, as long as you delete the identification from your records when you finish the verification process;
>
> f) answer a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or
>
> g) verify a picture of a driver's license of other photo ID submitted by the

[477] FEDERAL TRADE COMMISSION. **Children's Online Privacy Protection Rule**: A Six-Step Compliance Plan for Your Business. Available at: <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4> Accessed 16 Mar., 2022.

> parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.

There is much criticism of the inefficiency of legislation[478], especially because of the age verification problem, as children often lie about having access to a particular service that would not be available for their age group.

In 2014, it was found that a quarter of U.S. children between 8 and 12 years old used Facebook, although there is an express age limitation for people over 13 years of age. And the falsification often takes place with parental consent[479].

That is, the terms of consent signed by the parents do not guarantee the fidelity of age information and the protection of children as the norm implies.

The consent requirement, still, is subject to various exceptions. Essentially, consent is not required if the child's contact information is collected for the following reasons: to respond to a one-time specific request by a child; to obtain parental consent; or to protect the child's safety[480].

6.2.2 Information security

COPPA requires the website to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected about a child[481].

Specifically, this requires operators to develop policies and procedures to

---

[478]DOUGHERTY, Christie, Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU E-Privacy Regulation, 12 **NE. U. L. REV**. 629, 658 (2020); MATECKI, Lauren A., Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era, 5 **Nw. J.L. & SOC. POL'Y** 369, 370 (2010); PEASLEY, Mark. It's Time for an American (Data Protection) Revolution, 52 **AKRON L. REV**. 911, 943 (2018); SMITH, Nicole. Protecting Consumers in the Age of the Internet of Things, 93 ST. **JOHN'S L. REV**. 851, 866 (2019).

[479] AIKEN, Mary. **The Kids Who Lie About Their Age to Join Facebook**. The ATL. Available at: <https://www.theatlantic.com/technology/archive/2016/08/the-social-mediainvisibles/497729/> Accessed 09 Jul., 2021.

[480] § 6502(b)(1)(D)(2)(A)-(C). For example, if the only purpose for collecting a child's e-mail is for a one-time response to a request by a child for help with math homework, consent is not necessary. Other examples include mailing online newsletters and electronic postcards.

[481] 15 U.S.C. § 6502(b)(1)(D); 16 C.F.R. § 312.8.

protect children's personal information from "loss, misuse, unauthorized access, or disclosure"[482].

Recommended procedural safeguards include assigning an individual the responsibility of monitoring the security of the information, storing personal information on a secure server that is not accessible from the Internet, implementing access control procedures that require passwords, limiting employee access to the information, and deleting the information when it is no longer needed[483].

The FTC further recommends that Web site operators protect personal information in the possession of those who provide technical support for the internal operations of their sites. This could be achieved by incorporating specific contractual provisions that limit the contractors' ability to use the collected information[484].

6.2.3 Time and quality of information

As for the time of maintenance of the information, it determines the law that the operator shall retain personal information “for only as long as is reasonably necessary to fulfill the purpose for which the information was collected”[485]. After that, the information must be deleted to prevent unauthorized use or access, thus preserving the security of the information.

In any case, the quality of the data, when still relevant to the purpose of the collection, are subject to the parents review upon request[486]. Parents may, after being identified as such, even prohibit the future use of the data already collected and request the deletion of the data.

---

[482] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,906.
[483] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,906 nn.284 & 286.
[484] Children's Online Privacy Protection Rule, 64 Fed. Reg. at 59,906 nn.284 & 286.
[485] § 312.10 Data retention and deletion requirements.
[486] § 312.6 Right of parent to review personal information provided by a child.

6.2.4 Non-conditioning of the service to information other than those necessary for the operation of the same

Additional provisions of the COPPA prohibit a Web site from conditioning a child's participation in a game or receipt of a prize on his or her disclosure of more personal information than is reasonably necessary for the activity[487].

There is a similar device in the LGPD, which prohibits the conditioning of the participation of children in games or applications to the provision of personal information beyond those strictly necessary for the activity[488].

This prediction is especially relevant to the children's universe, since it is a marketing strategy to use "free" games that are ultimately remunerated for the collection of children's data.

6.2.5 Safe Harbor

COPPA[489] provides, in its final section, a self-regulatory guideline, issued by representatives of the marketing or online industries, or by the FTC. The Act directs the FTC to incorporate into its regulations incentives for operators to exercise self-regulatory guidelines that offer children the same protection as under the COPPA.

Some incentives for operators to implement self-regulations are:

(i) Mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines;

(iv) Referral to the [Federal Trade] Commission of operators who engage

---

[487] 15 U.S.C. § 6502(b)(1)(C).
[488] Art. 14, § 4, LGPD.
[489] 15 U.S.C. § 6503(b)(1).

> in a pattern of practice of violating the guidelines[490].

The FTC has the power to determine whether a particular website does indeed comply with the requirements of the COPPA.

The characteristics of self-regulation remain the same as those already addressed in Chapter 4, referring to attempts at transnational adequacy of data protection principles between the United States and the European Union through safe harbor.

6.3 The protection of children's data from dialogue with other internal sources

6.3.1 Comprehensive data protection

Especially since the 1990s, with the advancement of online marketing and data collection practices, privacy and data protection concerns have been growing in the United States. Unlike other countries, especially Europeans, privacy regulation in the United States was fragmented and without a national agency responsible for developing and enforcing policies[491].

The policy of the time, under Cliton's administration, was that the government should stay out of the nascent and pulsating industry so that innovation and e-commerce could flourish.

> For electronic commerce to flourish, the private sector must continue to lead. Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry.
>
> Accordingly, governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the

---

[490] 15 U.S.C. § 6503(b)(1).
[491] BENNETT, Colin. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data. **Technology and Privacy**: the new landscape. January 1997. Cambridge: MIT Press, p. 113.

Internet[492].

That is, the protection of privacy on the Internet, as well as e-commerce, should not be governed by laws, but by the industry itself from self-regulation.

However, the government was under increasing pressure from the European Union to establish data protection laws that were compatible with the criteria adopted by the EU's 1995 Data Protection Directive.

Safe harbor agreements are examples of this pressure and attempts to adjust to an adequate standard of protection for international data transactions.

Despite global pressure and the impacts that European regulations have had on companies around the world, it has not passed the U.S. Congress comprehensive federal data protection law so far. To date, COPPA remains the only US federal law specifically regulating consumer Internet privacy.

In any case, at the state level it is necessary to highlight the California Consumer Privacy Act (CCPA) [493] for being at the forefront in the data debate and protection[494].

The CCPA was a popular initiative designed to require the state of California to protect the privacy rights of state residents from intrusive business practices not explicitly prohibited by law.

It was the first comprehensive data privacy regulation in the United States designed to provide consumers with a data privacy framework involving transparency, control, and accountability.

---

[492] THE WHITE HOUSE. **A Framework for Global Electronic Commerce**. 1 July 1997. Available at: <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>. Accessed 11 May, 2022.

[493] Cal. Civ. Code § 1798, **California Consumer Privacy Act.** Available at: <http://leginfo.legislature.ca.gov/faces/codesdisplayText.xhtml?lawCode-CIV&division=3.&title=1.81.5.&part-4.&chapter=&article=> Accessed 12 Jul., 2021.

[494] Many academic papers analyze the norm and its influence: FREEMAN, Wilson C. California Dreamin' of Privacy Regulation: the California consumer privacy Act and congress. **Congressional Research Service**, 2018; JEEVANJEE, Kiran K., Nice Thought, Poor Execution: why the dormant commerce clause precludes California's CCPA from setting national privacy law, 70 **AM. U. L. REV**. F. 75, 2020; ALEXANDER, Christopher Bret. The General Data Protection Regulation and California Consumer Privacy Act: the economic impact and future of data privacy regulations, 32 **LOY. Consumer Rev.** 199. 2020; LI, Yunge. The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth, 32 **LOY. Consumer Rev.** 177, 2019.

Thus, it brought significant changes such as the right of access, right to be forgotten, right to choose not to have your information sold and right to receive equal service, even if choosing not to assign the data.

Since the enactment of the CCPA, California has inspired other states to pass similar regulations and several federal draft laws on the subject have passed, or have returned, to be discussed[495].

Nine states introduced bills after the CCPA on data privacy. Of these, six followed the specific language of the California standard for their own data protection laws: (Hawaii SB 418), Maryland (SB O613), Massachusetts (SD-341), Mississippi (HB 2153), New Mexico (SB 176), Rhode Island (S0234). The New York (S00224) and North Dakota (HB 1485) projects also contemplate some similarities, while Washington debates a data protection law model similar to GDPR.[496]

It remains to be remembered, as already dealt with in Chapters 1 and 2, that the U.S. Supreme Court understands that data protection, unlike privacy, is not an autonomous constitutional/fundamental right, but implicit in other safeguards.

6.3.2 Child protection

In 1989, world leaders made a commitment to children by adopting the United Nations Convention on the Rights of the Child: an international agreement on childhood that became the world's most comprehensive framework for the protection of children's rights.

It's also become the most widely ratified human rights treaty in history. Of the 196 participating members, only the United States of America did not ratify the document[497]. As they did not ratify any international human rights treaties since

---

[495] BINNIG, Christian F.; COMSTOCK, Christopher S., The California Consumer Privacy Act: the first step towards an american GDPR, **Infrastructure**, vol. 58, n. 4, summer 2019.

[496]MARMOR, Rachel R. et al., Copycat CCPA: bills introduced in states across country, **DAVIS WRIGHT TREMAINE LLP** (Feb. 8, 2019). Available at: <https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou> Accessed 12 Jul., 2021.

[497] UNITED NATIONS. **Convention on the Rights of the Child**. New York, 20 November 1989 STATUS AS AT: 24-07-2022 09:16:08 EDT. Available at:

December 2002, when it was ratified two optional protocols to the Convention on the Rights of the Child, about involvement of children in armed conflict and on the sale of children, child prostitution and child pornography[498].

In 1995, during the Clinton administration, the U.S. signed the treaty as a symbolic gesture of agreement with the principles set forth under the treaty. “But ratification of any treaty in the United States requires a two-thirds majority vote in the Senate to pass, several of Republican senators, claiming concerns about U.S. sovereignty, have consistently opposed ratification”[499].

Besides other obligations, ratification of the Convention would require the United States to submit reports, outlining its implementation on the domestic level, to the United Nations Committee on the Rights of the Child[500], a panel of child rights experts from around the world who monitors the implementation of the Convention by its States parties.

Although there is a portion of civil society that fights for ratification, and the promise of some governments to take the document to the Senate, there is great resistance from the conservative portion, for two important reasons: (i) the death penalty and life imprisonment and (ii) the parental rights.

About the first one, Article 37 of the Convention determines, among other things, that States Parties shall ensure that

> (a) No child shall be subjected to torture or other cruel, inhuman or degrading treatment or punishment. Neither capital punishment nor life imprisonment without possibility of release shall be imposed for offences

---

<https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2&mtdsg_no=IV-11&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.

[498] UNITED NATIONS. **Convention on the Rights of the Child**. New York, 20 November 1989 STATUS AS AT: 24-07-2022 09:16:08 EDT. Available at: <https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2&mtdsg_no=IV-11&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.; UNITED NATIONS. **Convention on the Rights of the Child**. New York, 25 May 2000, 11.c Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Available at: <https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2&mtdsg_no=IV-11-c&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.

[499] ATTIAH, Karen. Why won’t the U.S. ratify the U.N.’s child rights treaty? **The Washington Post.** November 21, 2014 at 4:12 p.m. EST. Available at: <https://www.washingtonpost.com/blogs/post-partisan/wp/2014/11/21/why-wont-the-u-s-ratify-the-u-n-s-child-rights-treaty/> Accessed 24 Jul., 2022.

[500] UNITED NATIONS. **Committee on the Rights of the Child**. Available at: <https://www.ohchr.org/en/treaty-bodies/crc> Accessed 24 Jul., 2022.

committed by persons below eighteen years of age [...].

Considering that the document was introduced in 1990, The United States did not comply with this article at the time.

It was only in 2005 that the U.S. Supreme Court ruled that the use of the death penalty against juvenile offenders aged 17 or younger is cruel and unusual punishment prohibited by the Eighth Amendment[501].

And in 2010 that a life imprisonment was forbidden without the possibility of parole for non-homicide crimes[502]. Homicide crimes were included in the impossibility of mandatory sentences of life without the possibility of parole for juvenile murderers, in a 2012 decision[503].

The second point, and probably the most important in relation to the understanding of child protection in the United States and the contrast with Brazil is in the idea of "parental rights".

This expression is not even used in Brazil from the perspective of child protection. On the contrary, the Statute of the Child and Adolescent provides for rights only for children and adolescents. While parents are entrusted with responsibilities and obligations to ensure the welfare of minors.

However, opponents of Us ratification are based on the argument that the authority of parents would be subverted. This current can be exemplified by the ParentalRights.Org: protecting children by empowering parents, led by constitutionalist lawyer Michael P. Farris, that has been actively campaigning against U.S. ratification.

The reasons would be, briefly, three: (a) the first is about the idea of "the best interest of the child" being first considered. Therefore, who would decide on what is the best interest of the child would be the government and not the parents; (b) unchecked authority in deciding what the treaty does or does not mean and what

---

[501] Roper v. Simmons, 543 U.S. 551 (2005).
[502] Graham v. Florida, 560 U.S. 48 (2010)
[503] Miller v. Alabama, 567 U.S. 460 (2012).

nations must do to be in compliance; and (c) in America would have the effect of passing a massive new federal law on the family, giving to the Congress the power to do so[504].

At all these points what can be seen is the concern to decrease the authority of parents and give it to the State to decide what would be appropriate in the protection of the child.

> The group fears that ratifying the treaty would mean children could choose their own religion, that children would have a legally enforceable right to leisure, that nations would have to spend more on children's welfare than national defense, and that a child's "right to be heard" could trigger a governmental review of any decision a parent made that a child didn't like[505].

That is, a fear of state intervention in family relationships, especially parents with their children, removing the power of supreme authority in decisions on the welfare of children.

Another point that can also be observed is that the country "remains the only high-income nation in the world without national paid maternity or parental leave. Parental leave, both maternal and paternal, is critical to a child's health, development and wellness"[506]. Ratification of the declaration would impose internal adjustments to this effect.

Ratifying the convention would mean adapting the internal rules to the principles of that convention and concretizing them through public policies, something that the Senate has so far failed to approve with the necessary amount of votes.

---

[504] PARENTALRIGHTS. **The Convention on the Rights of the Child Is Back in Congress**. March 3, 2020. Available at: <https://parentalrights.org/convention-on-the-rights-back/> Accessed 06 Aug., 2022.

[505] ATTIAH, Karen. Why won't the U.S. ratify the U.N.'s child rights treaty? **The Washington Post**. November 21, 2014. Available at: <https://www.washingtonpost.com/blogs/post-partisan/wp/2014/11/21/why-wont-the-u-s-ratify-the-u-n-s-child-rights-treaty/> Accessed 06 Ago., 2022.

[506] UCLA Fielding School of Public Health. **A global report card**: Are children better off than they were 25 years ago? Available at: <https://ph.ucla.edu/news/press-release/2014/nov/global-report-card-are-children-better-they-were-25-years-ago> Accessed 25 Jul., 2022.

6.3.3 Protection against advertising

Under COPPA, except in very specific cases, it is necessary to obtain verified parental consent before collection through one of the forms included in the document.

The need to have consent before collecting/using any information from a child, which includes, as seen, browsing data or other browsing information, makes it difficult, in practice, advertise strategies that rely on behavioral targeting.

Thus, COPPA does not theoretically prohibit the use of behavioral advertising, retargeting or user profiling for advertising; but given the difficulty of obtaining consent from parents on a large scale, in practice, it becomes almost impossible to adapt to the norm in these cases.

The best way to address advertising to children without confronting COPPA would be through zero-data strategies. That is, without collecting user-specific data to deliver advertising material.

In order for advertising to reach its purpose, strategies are restricted to those that do not require individualized profiles and seek, through the content to reach the target audience, as happens in contextual basis only advertising.

So, if a website, app, or even a section a site, or any kind of online service is targeted to appeal to children, then it is considered child-directed, and should treat every visitor to this service as if they are a child and comply with COPPA. “Classifying a service as child-directed is subjective but requires consideration of factors such as whether it features characters popular with kids, vocabulary intended for kids, products that are appealing to kids, etc”[507].

Many have classified their content as general audience, even if in practice they also reach children, to try to circumvent the restrictions brought to children's

---

[507] INTERACTIVE ADVERTISING BUREAU. **Guide to navigating COPPA**: recommendations for compliance in an increasingly regulated children's media environment. October 2019, p. 7. Available at: <https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf> Accessed 17 Jul., 2022.

content, which do not exist if the content is addressed to the general public.

This practice, when made in order to circumvent the restrictions, has been the subject of investigations and severe fines by the FTC, as will be seen in the next item.

There is also a specific Safe Habor program under COPPA, for children's advertising, called "The Children's Advertising Review Unit" (CARU), that "helps companies comply with laws and guidelines that protect children under age 13 from deceptive or inappropriate advertising and ensure that, in an online environment, children's data is collected and handled responsibly"[508].

The program brings in its guideline[509] specific definitions to avoid deceptive or unfair advertising to children whom it is directed.

CARU guidelines are divided into nine categories: Deception; Product Presentations and Claims; Material Disclosures and Disclaimers; Endorsements; Blurring of Advertising and Editorial/Program Content; Premiums; Kids' Clubs; Sweepstakes and Contests; Online Sales; Sales Pressure; and Unsafe and Inappropriate Advertising to Children.

The protection and guarantee of children's rights in relation to advertising is based on the idea of accountability of those who advertise for the protection of the child, as well as on the recognition that "children have limited knowledge, experience, sophistication, and maturity"[510], therefore,

> advertisers should recognize that younger children have a limited capacity to evaluate the credibility of information, may not understand the persuasive intent of advertising, and may not even understand that they are viewing or hearing advertising[511].

---

[508] BBB National Programs. **Children's Advertising Review Unit (CARU).** Available at: <https://bbbprograms.org/programs/all-programs/children's-advertising-review-unit> Accessed 17 Jul., 2022.

[509] BBB National Programs. **Children's Advertising Review Unit (CARU).** Self-Regulatory Guidelines for Children's Advertising. Available at: <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf> Accessed 17 Jul., 2022.

[510] BBB National Programs. **Children's Advertising Review Unit (CARU).** Self-Regulatory Guidelines For Children's Advertising. Available at: <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf> Accessed 17 Jul., 2022.

[511] BBB National Programs. **Children's Advertising Review Unit (CARU).** Self-Regulatory Guidelines

This recognition of children's hypervulnerability to advertising is essential for protecting them and conduct guidelines for advertisers.

It is also recognized that the social and personal development of children is the primary responsibility of parents and that advertisers should not undermine this relationship.

Furthermore, advertising should serve as a positive influence of qualities and behaviors for children, such as "taking safety precautions, and engaging in physical activity", as well as encouraging healthy development, human diversity and respect[512].

Another regulation comes from the Federal Communication Commission (FCC), which aims to regulate commerce in telephone, radio and TV communication. The government agency has the responsibility to administer the process of granting broadcast licenses and evaluate the performance of a broadcaster for the purpose of renewing its license.

Therefore, it has set advertising time limits, through the Children's Television Act of 1990[513], for children's programs: no open or cable TV station should broadcast more than 10 minutes and 30 seconds of advertising per hour during children's programming on weekends; or more than 12 minutes per hour during the week. Furthermore, “FCC also requires this program material be separated from commercials by intervening and unrelated program material”[514].

It is concluded, then, that the regulation of children's advertising is restricted to television, through the FCC, or self-regulation, through CARU; but in both cases under the COPPA rule.

---

for Children’s Advertising. Available at: <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf> Accessed 17 Jul., 2022.

[512]BBB National Programs. **Children's Advertising Review Unit (CARU).** Self-Regulatory Guidelines For Children's Advertising. Available at: <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf> Accessed 17 Jul., 2022.

[513] H.R.1677 - **Children's Television Act of 1990**. Available at: <https://www.congress.gov/bill/101st-congress/house-bill/1677> Accessed 18 Jul., 2022.

[514] FEDERAL COMMUNICATION COMMISSION. **Children's Educational Television.** Available at: <https://www.fcc.gov/consumers/guides/childrens-educational-television> Accessed 18 Jul., 2022.

6.4 FTC and the COPPA enforcement

Originally established by the Federal Trade Commission Act (FTCA) in 1914 to eliminate and prevent anticompetitive business practices, the FTC has expanded its responsibility to promote consumer protection from a wide variety of specific norms[515].

The FTCA authorizes the FTC to prevent "unjust or deceptive acts" that affect trade. Through this clause, the Commission is authorized to impose and process sanctions as well as regulate norms.[516]

The Federal Trade Commission (FTC) has the power to enforce the COPPA and has developed regulations to implement its requirements, which became effective on April 21, 2000.

Parents, consumer groups, industry members, and others that believe an operator is violating COPPA may report that to the FTC, as the implementing agency, that has the authority to take direct action to enforce the statute's requirements.

One benefit given to the regulation of child data is the exception procedure called APA. According to the Administrative Procedure Act (APA)[517], the regulatory process becomes more simplified, by which the agency publishes a proposed rule, accepts public comments, and then publishes the final version.

This agility has the benefit of providing the constant updating of the law, as was done in 2010 in response to the new realities of use of social networks and applications[518]. From the review it was considered an expansion of the concept of

---

[515] FEDERAL TRADE COMMISSION. **A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority**. July 2018. Available at: <https://www.ftc.gov/about-ftc/mission/enforcement-authority> Accessed 09 Jul., 2021.

[516] O'REILLY, James. **FEDERAL PREEMPTION OF STATE AND LOCAL LAW**: legislation, regulation, and litigation 8 (2006), Available at: <http://apps.americanbar.org/abastore/products/books/abstracts/5010047samplechpabs.pdf> Accessed 09 Jul., 2021.

[517] ELECTRONIC PRIVACY INFORMATION CENTER. **The Administrative Procedure Act (APA).** Available at: <https://www.justice.gov/sites/default/files/jmd/legacy/2014/05/01/act-pl79-404.pdf> Accessed 09 Jul., 2021.

[518]FEDERAL TRADE COMMISSION. **Statement of Basis and Purpose on Children's Online Privacy Protection Rule Final Rule**, 78 Fed. Reg. No. 12 3972-2996 (Jan. 17, 2013). Available at: <https://www.ftc.gov/system/files/2012-31341.pdf> Accessed 09 Jul., 2021.

"personal information", to include the names or surnames used for identification, individualized addresses of computers (such as IPs), geolocation, photos, videos and audio recording.

The revised norm recognized that, although in the 1990s it was not possible to contact a person only by disclosing their photo, today, clearly, it is.

There are even more informal ways in which the agency updates the interpretations given to the standard, such as the "Online FAQs": a kind of question-and-answer organization that brings a guide for parents and companies on the practices expected to better adapt to COPPA.

Blogging, workshops and other methods are also considered appropriate and allow the Commission to be more agile in terms of updating the guidelines, although the ability to coerce these informal parameters is questionable.

Decisions can only be reviewed by collegiate decision after listening to the independent sector regulatory agency in order to assure the agency's independence.

Law enforcement is a key aspect. In this sense, COPPA does not provide for the individual and private right of action, leaving only the State the role of investigating, promoting, and implementing sanctions. This is done mainly through the Federal Trade Commission and state attorneys.

COPPA also gives states and certain federal agencies authority to enforce compliance with respect to entities over which they have jurisdiction.

> For example, New York has brought several COPPA enforcement actions. (…) In addition, some federal agencies, such as the Office of the Comptroller of the Currency and the Department of Transportation, are responsible for handling COPPA compliance for the specific industries they regulate[519].

Foreign-based websites must also comply with COPPA as do U.S.-based websites that collect information from foreign children. Many of the cases addressed in the following item refer to foreign-bases websites, as will be seen.

---

[519] FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions, FED. TRADE COMM'N § B(3) (July 2020), Available at: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>. Accessed 04 May, 2022.

6.4.1 Penalties

Violators of COPPA can be liable for civil penalties up to 43,280 USD[520] per violation depending on

> the egregiousness of the violations, whether the operator has previously violated [COPPA], the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company[521].

In consultation with the FTC website, in the library of "cases"[522], it is possible to view 5102 Cases and Proceedings, of which only 74 refer to the protection of children's privacy.

Restricted only to cases after the revision of the 2012 standard, there are:

1. Kuuhuub, Inc., et al., U.S. v. (Recolor Oy) (July 22, 2021)

   Civil Penalty: $3,000,000

   Case Summary: Kuuhuub Inc., Kuu Hubb Oy and Recolor Oy settled FTC allegations that they violated a children's privacy law by collecting and disclosing personal information about children who used the app without notifying their parents and obtaining their consent[523].

2. Miniclip, In the Matter of (July 6, 2020)

   Case Summary: In May 2020, the Commission accepted for public comment a proposed consent agreement to resolve allegations that Miniclip S.A. violated Section 5 of the FTC Act by misrepresenting its status in a Children's Online Privacy Protection Act ("COPPA") safe harbor program[524].

3. HyperBeard, Inc. (June 4, 2020)

---

[520] FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions, FED. TRADE COMM'N § B(3) (July 2020), Available at: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>. Accessed 04 May, 2022.

[521] FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions, FED. TRADE COMM'N § B(3) (July 2020), Available at: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>. Accessed 04 May, 2022.

[522] FEDERAL TRADE COMMISSION. **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings> Accessed 04 May, 2022.

[523] FEDERAL TRADE COMMISSION. **Legal Library:** Cases and Proceedings Available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3184-kuuhuub-inc-et-al-us-v-recolor-oy> Accessed 04 May, 2022.

[524] FEDERAL TRADE COMMISSION. **Legal Library:** Cases and Proceedings Available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3129-miniclip-matter> Accessed 04 May, 2022.

Civil Penalty: $150,000

Case Summary: HyperBeard, a developer of apps that are popular with children has agreed to pay $150,000 and to delete personal information it illegally collected from children under 13 to settle Federal Trade Commission allegations. In a complaint filed by the Department of Justice on behalf of the FTC, the Commission alleges that HyperBeard, Inc. violated the Children's Online Privacy Protection Act Rule (COPPA Rule) by allowing third-party ad networks to collect personal information in the form of persistent identifiers to track users of the company's child-directed apps, without notifying parents or obtaining verifiable parental consent. The ad networks used the identifiers to target ads to children using HyperBeard's apps[525].

4. Google LLC and YouTube, LLC (September 4, 2019)[526]

Civil Penalty: $170,000,000

Case Summary: Google LLC and its subsidiary YouTube, LLC agreed to pay a $170 million civil penalty to the Federal Trade Commission and the New York Attorney General to settle allegations that the YouTube video sharing service illegally collected personal information from children without their parents' consent in violation of the Children's Online Privacy Protection Act Rule (COPPA)[527].

5. Unixiz, Inc. doing business as i-Dressup.com (April 24, 2019)

Civil Penalty: $35,000

Case Summary: Unixiz, Inc., doing business as i-Dressup.com, and the individually named defendants CEO Zhijun Liu and Secretary Xichen Zhang, reached a settlement over allegations they violated the Children's Online Privacy Protection Act (COPPA)[528].

6. Musical.ly, Inc. (February 27, 2019)

Civil Penalty: $5,700,000

Case Summary: Video social networking app Musical.ly, Inc., now known as TikTok, agreed to pay $5.7 million to settle Federal Trade Commission allegations that the company illegally collected personal information from

---

[525] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3109-hyperbeard-inc> Accessed 04 May, 2022.

[526] This case will be better examined in the following chapter as an example of transnationality of the effects of the agreement.

[527] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-YouTube-llc> Accessed 04 May, 2022.

[528] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings. Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3002-unixiz-inc-doing-business-i-dressupcom> Accessed 04 May, 2022.

children in violation of the Children's Online Privacy Protection Act. [529].

7. Prime Sites, Inc. (Explore Talent) (February 12, 2018)

Civil Penalty: $235,000

Case Summary: The FTC's complaint against Nevada-based Prime Sites, Inc. alleges that the company – doing business as Explore Talent – violated the Children's Online Privacy Protection Act (COPPA) by collecting and disclosing children's personal information without obtaining parental consent and by failing to detail to parents and the public its collection, use, and disclosure practices. The complaint also alleges that the company violated the FTC Act by baselessly representing to prospective purchasers of its premium services that casting directors either had interest in them or had specifically chosen them for upcoming roles[530].

8. VTech Electronics Limited (January 8, 2018)

Civil Penalty: $650,000

Case Summary: Electronic toy manufacturer VTech Electronics Limited and its U.S. subsidiary have agreed to settle charges by the Federal Trade Commission that the company violated a U.S. children's privacy law by collecting personal information from children without providing direct notice and obtaining their parent's consent, and failing to take reasonable steps to secure the data it collected[531].

9. InMobi Pte Ltd. (June 22, 2016)

Civil Penalty: $950,000

Case Summary: Singapore-based mobile advertising company InMobi will pay $950,000 in civil penalties and implement a comprehensive privacy program to settle Federal Trade Commission charges it deceptively tracked the locations of hundreds of millions of consumers – including children – without their knowledge or consent to serve them geo-targeted advertising[532].

10. Retro Dreamer (December 17, 2015)

---

[529] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3004-musically-inc> Accessed 04 May, 2022.
[530] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3218-prime-sites-inc-explore-talent> Accessed 04 May, 2022.
[531] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3032-vtech-electronics-limited> Accessed 04 May, 2022.
[532] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3203-inmobi-pte-ltd> Accessed 04 May, 2022.

Civil Penalty: $360,000

Case Summary: These cases are the first in which the FTC alleged that companies allowed advertisers to use persistent identifiers to serve advertising to children. Persistent identifiers – pieces of data that are tied to a particular user or device – were among the categories added to the COPPA Rule's definition of personal information when it was updated in 2013[533].

11. TinyCo, Inc. (September 17, 2014)

Civil Penalty: $450,000 and $300,000

Case Summary: Online review site Yelp, Inc., and mobile app developer TinyCo, Inc., agreed to settle separate Federal Trade Commission charges that they improperly collected children's information in violation of the Children's Online Privacy Protection Act, or COPPA, Rule[534].

12. Path, Inc. (February 1, 2013)

Civil Penalty: $800,000

Case Summary: The operator of the Path social networking app has agreed to settle Federal Trade Commission charges that it deceived users by collecting personal information from their mobile device address books without their knowledge and consent. The settlement requires Path, Inc. to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for the next 20 years[535].

13. Artist Arena LLC, United States of America (for the Federal Trade Commission) (October 4, 2012)

Civil Penalty: $1,000,000

Case Summary: The operator of fan websites for music stars Justin Bieber, Rihanna, Demi Lovato, and Selena Gomez has agreed to settle Federal Trade Commission charges that it violated the Children's Online Privacy Protection Act (COPPA) by improperly collecting personal information from

---

[533] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/142-3261-lai-systems-llc> and <https://www.ftc.gov/legal-library/browse/cases-proceedings/142-3262-retro-dreamer> Accessed 04 May, 2022.

[534] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3066-yelp-inc> and <https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3209-tinyco-inc> Accessed 04 May, 2022.

[535] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3158-path-inc> Accessed 04 May, 2022.

children under 13 without their parents' consent[536].

14. RockYou, Inc. (March 27, 2012)

Civil Penalty: $250,000

Case Summary: The operator of a social game site has agreed to settle charges that, while touting its security features, it failed to protect the privacy of its users, allowing hackers to access the personal information of 32 million users. The Federal Trade Commission also alleged in its complaint against RockYou that RockYou violated the Children's Online Privacy Protection Act Rule (COPPA Rule) in collecting information from approximately 179,000 children. The proposed FTC settlement order with the company bars future deceptive claims by the company regarding privacy and data security, requires it to implement and maintain a data security program, bars future violations of the COPPA Rule, and requires it to pay a $250,000 civil penalty to settle the COPPA charges[537].

15. Godwin, Jones O., d/b/a skidekids.com (November 8, 2011)

Case Summary: The operator of www.skidekids.com, a website that advertises itself as the "Facebook and Myspace for Kids," has agreed to settle Federal Trade Commission charges that he collected personally information from approximately 5,600 children without obtaining prior parental consent, in violation of the Commission's Children's Online Privacy Protection Act ("COPPA") Rule[538].

16. W3 Innovations, LLC d/b/a Broken Thumb Apps and Justin Maples, U.S. (September 8, 2011)

Civil Penalty: $50,000

Case Summary: A developer of mobile applications, including children's games for the iPhone and iPod touch, will pay $50,000 to settle Federal Trade Commission charges that it violated the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule by illegally collecting and disclosing personal information from tens of thousands of children under age 13 without their parents' prior consent. This is the Commission's first case involving mobile applications, known as apps[539].

---

[536] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/112-3167-artist-arena-llc-united-states-america-federal-trade-commission> Accessed 04 May, 2022.

[537] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/1023120-rockyou-inc> Accessed 04 May, 2022.

[538] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/1123033-godwin-jones-o-dba-skidekidscom> Accessed 04 May, 2022.

[539] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings

17. Playdom, Inc. (May 12, 2011)

> Civil Penalty: $3,000,000
>
> Case Summary: The operators of 20 online virtual worlds have agreed to pay $3 million to settle Federal Trade Commission charges that they violated the Children's Online Privacy Protection Rule by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' prior consent. This settlement is the largest civil penalty for a violation of the FTC's COPPA Rule[540].

18. Iconix Brand Group, Inc. (October 20, 2009)

> Civil Penalty: $250,000
>
> Case Summary: Iconix required consumers on many of its brand-specific Web sites to provide personal information, such as full name, e-mail address, zip code, and in some cases mailing address, gender, and phone number – as well as date of birth – in order to receive brand updates, enter sweepstakes contests, and participate in interactive brand-awareness campaigns and other Web site features[541].

As highlighted in topic 6.2.1, U.S. child privacy protection regulations gravitate around parental consent. Thus, almost all penalties refer to failure to obtain consent as a way of not complying with the rules imposed.

The second hypothesis of application was in the request for data for participation in games or other types of interactions, which is forbidden by COPPA, as so by LGPD, as seen.

Otherwise, other possible offenses to child privacy, when consented by parents, are discovered of practical protection. In this sense, the Brazilian legislation is broader and offers greater interpretative possibility of protection not only to the data, but from other values linked to it, such as privacy – after the best interest of the child.

The specific objective of chapter 6 is then concluded, namely, to take over

---

Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/102-3251-w3-innovations-llc-dba-broken-thumb-apps-justin-maples-us> Accessed 04 May, 2022.

[540] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/1023036-playdom-inc> Accessed 04 May, 2022.

[541] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; **Legal Library:** Cases and Proceedings Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/iconix-brand-group-inc> Accessed 04 May, 2022.

the protection of children's data from the American legal system, confronting, when possible, to the Brazilian legal system.

It will be up to the next, and last chapter, to establish the protection of children's data on the basis of transnational criteria.

CHAPTER 7
THE PROTECTION OF CHILDREN'S DATA FOR COMMERCIAL PURPOSES IN BRAZIL FROM TRANSNATIONAL STANDARDS

7.1 Necessary transnational approach to the implementation of child data protection for commercial purposes

The United States has opted for a specific child data protection law. However, the U.S. country does not have general data protection regulations at the federal level, as already addressed.

Brazil, on the contrary, sanctioned in 2018, after eight years of debates, the General Data Protection Law, but dealt in only one article (art. 14) the specificities of the processing of children's data.

However, given the little experience of applying the law, there are still no specific parameters of how the interpretation or even regulation of it will be. The originality of the dissertation consists in sustaining the application of a transnational criterion in the implementation of data protection and the privacy of children in Brazil.

As seen, data protection legislation is essential to protect the interest of individuals who can no longer control the use made of their personal information. The international nature of data protection necessitates a harmonized approach by all countries involved.

International expectations increasingly put pressure on countries without data protection legislation to adopt such legislation if they wish to remain part of the international information community. Despite differences in language, legal traditions and cultural and social values, there has been a broad measure of agreement on the basic principles that should be embodied in data protection legislation.

Bennett[542] noted the trend of convergence in public policies related to data protection in comparative law, as a dynamic process shaped by different forces. They would be (i) technological determinism, as a pattern generated by the pioneers and followed by the other; (ii) emulation, in adopting the standards already existing in other countries; (iii) the existence of an elite group, being specialized professionals who participate in various proposals in different countries; (iv) the harmonization of a cohesive policy and (v) penetration, as a permeability of one jurisdiction to receive reflections of procedures of another.

This analysis justifies the necessary observance of data protection beyond national borders in this work. The convergence of principled values, beyond similarity, proposes an important dialectic in the construction of instruments and tools to protect these[543].

In the second item of this chapter what will be proposed is to identify which convergences of these can be adopted by Brazil in harmony with what already exists in the country.

For this first subtopic, it will be explored how the standards already established transnationally can permeate the Brazilian jurisdiction.

In addition to a systematic interpretation from the internal legal system, considering the Federal Constitution, The Statute of the Child and Adolescent and the Consumer Protection Code, for example**,** new global actors delimit, in practice, how the data of millions of children are treated.

Thus, to understand the new arrangements of power, and, consequently, who produces the protection criteria, it is based on the understanding that:

> this new legal paradigm permeates the state normative tissues, using the channels that globalization itself creates (in primis those economic and judicial) and subtracting sovereignty from "traditional" institutions. It is the "language of interests", therefore, to make the boundary between hard law (Constitution, laws, etc.) and soft law (judicial background, "structural adjustment programs of state finances", etc.) become ever more subtle and

---

[542] BENNETT, Colin. **Regulating privacy**: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992, p. 116-152.
[543] BENNET, Colin; RAAB, Charles. **The Governance of Privacy**: Policy Instruments in the Digital Age, MIT University Press, 2006.

> irrelevant. The transnational normative language is declared more as an engine of "convergences" and "dialogues" than of differences (...)[544] (free translation).

The role of transnational companies[545], especially in the data protection category, is crucial. It is these private actors who hold the greatest power over the technologies that collect and treat information about the behavior of individuals on the Internet, from business models that presuppose data monetization and behavioral modulation, for commercial purposes.

From Cassesse, in his question that makes the title to the work "Chi governa il mondo?", it is possible to understand the globally diluted scenario in which cooperation between agents predominates, and overcomes those who dominate [546]*the network* and establishes a direct connection with civil society, breaking the monopoly of the State.[547]

And it is these large companies, which have almost a monopoly on social networks and large accumulations of data, that dominate the direct connection with society.

In this sense, globalization brings the change of power to new actors. "Ideological, institutional and normative power, with the respective social interactions that at all times find new arrangements" (free translation)[548].

Composed of public-private hybrid matrix standardization bodies, that create bridges between public and private sectors, but with public regulatory

---

[544]OLIVIERO, Maurizio; CRUZ, Paulo Márcio. Reflections on transnational law. **New Legal Studies Journal.** Itajaí, v. 17, n. 1, p. 18-28, 2012. See also CRUZ, Paulo Márcio & BODNAR, Zenildo. The new paradigm of law in postmodernity. Porto Alegre - RECHTD/UNISINOS. **Journal of Constitutional Studies, Hermeneutics and Theory of Law**, v. 3, p. 75-83, 2011 and CRUZ, Paulo Márcio; FERRER, G. R. Soberanía y transnacionalidad: antagonismos y consecuencias. Barcelona - Revista de Derecho - España. **Revista de Derecho vLex**, v. 63, p. 1-., 2008.

[545] Although there is no peaceful delimitation in the doctrine on the operational concept of the Transnational Company, in this work will be adopted the one from ZUBIZARRETA, Juan Hernández. **Las empresas transnacionales frente a los derechos humanos**: história de una asimetría normativa. Bilbao: Hegoa, 2009.

[546]CASSESE, Sabino. **Chi governa il mondo?** Bologna: Il Mulino, 2013.

[547]CASSESE, Sabino. **Chi governa il mondo?** Bologna: Il Mulino, 2013, p. 35.

[548]STAFFEN, Ricardo Márcio. **Interfaces of Global Law.** 2. Ed. Ampl. current. Rio de Janeiro: Lumen Juris, 2018, p. 23.

attributions; as well as strictly private organizations[549], the global scenario is complex.

For this study, it was chosen to use, as “standard” the same reference that Frydman[550] brings in his work "The end of the rule of law: governing by standards and indicators", which "designates, at the same time, both the technical standard and the ISO standard, for example, as the model (of behavior or an object, of standard (of measure) or of benchmark (reference level)".

Thus, unlike the rules, being those classical legal sources, the standards are derived from technical standards produced by a growing number of sources, public and private, national, regional, and global. Sometimes law ends up resorting to technical norms in an auxiliary way to normativity. As an example, the author cites the definition of a tolerable noise limit, in which the legislator himself or regulatory authorities will integrate references to technical standards in order to complement or detail legal regulations[551].

However, the apparently existing dichotomy that technical norms standardize things, while legal norms determine behavior and relationships between people, does not resist to theoretical approach and

> it becomes unsustainable when the 'things' that are intended to be managed are no longer products, but services, that is, human activities, and technical standards become management standards and management tools[552].

Thus, in the normative field, the author classifies the standardization of things and processes (and through compliance with these standards) as technical standards and standards aimed at the conduct of people as management standards[553]; that intertwine and blend with each other.

---

[549] CASSESE, Sabino. **Chi governa il mondo?** Bologna: Il Mulino, 2013, p. 19.
[550] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 19-20.
[551] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 20-21.
[552] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 25.
[553] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation

Technical norms are still "legal norms, by which the political authority imposes a certain behavior on the recipients"[554], however, their source of derivation is mainly the scientific observation of experiments. It is therefore "a kind of hybrid legislation, which ensure a form of mediation between scientific laws and legal rules"[555].

These survived the liberal ideas resulting from the industrial revolution of the 19th century, in which it came not to accept state management in the economy[556]. For how much they were considered of bilateral interest, in the sense that, for example, engineers go to engineers, stipulating criteria and better forms of performance. In other words, one relies on technique beyond the political issue.

And, as a result of the same revolution are the embryonic "risk society" arising from[557] the massification of production and the need to establish technical standards that not only protect the industry itself, but that inform the consumer of the form of use, care and other necessary prescriptions.

Classical legal rules operate in increasing competition with technical and management standards, both within states and in the transnational context.

Especially in recent decades, globalization has brought an "irresistible extension of the mastery of the technical standard"[558], observed through the "laboratory of globalization" that is the European Union. Standards gain systematization in this new state of things. Overcoming customs barriers, the next was the removal of technical obstacles, through standardizations and directives to eliminate and standardize procedures, techniques, and visions legally and in a

---

of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 17-28.
[554] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 25.
[555] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 24.
[556] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 31-35.
[557] Term coined by Ulrich Beck.
[558] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 26.

different way, until then, by the Member States.

Thus, products and services, to circulate in the block, began to meet the essential requirements regarding health, safety, environment, among other criteria defined in the standards.

> From this new approach, it is clear from there that they are European or international technical standards, and no longer national laws, not even EU law, in the strict sense, which lay down, in practice and specifically, the requirements to be respected in the field of health, safety and the environment, for almost all products and services that circulate and are marketed in the European Union[559].

It is not merely the exchange of legal rules for technical norms, but a structural change in the domain of normativity production, leaving the rule of law to the domain of standardization; since the standards are not drawn up by traditional political bodies, "but within CEN, ISO, or specialized sectoral bodies"[560].

In the current global scenario, rules on data protection, environment, industrial property, international contracts, investments, justice systems, the functioning of capital markets and international financing based on risk assessment by specialized agencies are just a few examples of the interrelationship between these two major groups of rules: technical and management standards, state legal systems on the other.

These are complex issues that require immediate rule on highly specialized issues and that call into question the state's ability to bring answers within its legislative processes.

So, Frydman brings a strict concept of "standards" as rules created by private institutions, devoid of political responsibility (accountability), and without state participation, which condition the behavior of the State and the individual, generating a real tension by the lack of sovereign acts in the participation of norms increasingly

---

[559] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 59.
[560] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 59.

present in world society[561].

This is the best approximation of the concept of standard used in this dissertation. However, not only rules created by private institutions, but also created by States that will be considered as standard when applied outside their jurisdiction. This is the obvious case of COPPA, which has become a standard because it has influence not only in the United States, but also in the creation and implementation of standards by other public and private entities around the world.

A case deserves special attention: FTC versus YouTube. First, because it was the largest deal ever made by the Commission[562], in one hundred and seventy million dollars, and second, because YouTube is the second most visited site in the world, behind only from Google[563].

Furthermore, this is an example of great importance because it is the application currently most accessed by children, both in Brazil[564] and in the United States[565]. Thus, in addition to the obvious impacts, the agreement can be considered a criterion for other applications that also target children.

With the supposed protection of free trade in the U.S. territory, where most companies are headquartered, and under the argument that digital platforms were not designed for children under the age of 13, they ignored compliance with data protection standards.

Until 2020, two decades after COPPA came into force, no U.S. company,

---

[561] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018.

[562] Until then, the case for the largest deal was FTC x Musical.ly (now Tiktok), at five million seven hundred thousand dollars.

[563] SIMILARWEB. **Top Websites Ranking.** Available at: <https://www.similarweb.com/top-websites/> Accessed 09 Jul., 2021. Ranking method can be found at: <https://www.similarweb.com/corp/ourdata/> Accessed 09 Jul., 2021.

[564]As for the use of apps by age: YouTube Kids: 0-3 years 69%, 4-6 years old 71%, 7-9 years old 55% and 10-12 years old 34%. YouTube 0-3 years old 59%, 4-6 years old 63%, 7-9 years old 77% and 10-12 years old; 82% of children accessthe app. PANORAMA MOBILE TIME/OPINION BOX. **Children and smartphones in Brazil.** October 2019. Available at: <https://www.mobiletime.com.br/research/children-and-smartphones-no-brasil-Oct-de-2019/> Accessed 29 Jun., 2021.

[565] Among the evidence presented in the lawsuit, the FTC used presentations by Google executives to toy industry customers in which YouTube is considered the "number 1 website regularly visited by children." Available at <https://www.ftc.gov/system/files/documents/cases/YouTube_complaint_exhibits.pdf> Accessed 29 Jun., 2021.

investigated by the regulatory body, FTC (*Federal Trade Commission),* was brought to court for the violations[566]. However, the thirty companies investigated made agreements with the Commission.

As occurred when the FTC sanctioned YouTube for improperly collecting data on videos made for children, to offer advertisements specifically targeted at children, and thus infringing on COPPA[567]. The collection of information would only be permitted by express consent of parents or legal guardians, which YouTube failed to obtain.

The defense insisted that the platform was aimed at a general public and not children, and therefore would not require COPPA compliance. However, evidence gathered by the agency showed that, in presentations directed at advertisers, the company positioned itself as: “today's leader in reaching children age 6-11 against top TV channels”; “unanimously voted as the favorite website of kids 2 – 12”; “93% of tweens visit YouTube to watch videos”; “it's the #1 website regularly visited by kids”; “#1 source where children discover new toys+ games”; “The new "Saturday Morning Cartoons": 41% of parents watch family content on YouTube together with their children”[568].

On the other hand, the FTC considered that even if the platform was not intended for children, because it was aware of the use by the ones under the age of 13, YouTube would be subject to the rules of the specific law[569].

---

[566]States can, and have, sued companies according to COPPA, but the FTC controls the vast majority of enforcement actions. FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions. Available at: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> Accessed 09 Jul., 2021.

[567]FEDERAL TRADE COMMISSION. **Google LLC and YouTube, LLC.** Available at: <https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-YouTube-llc> Accessed 09 Jul., 2021.

[568] FEDERAL TRADE COMMISSION. **Complaint Exhibits A - C**. Case 1:19-cv-02642 Document 1-1 Filed 09/04/19. Available at: <https://www.ftc.gov/system/files/documents/cases/YouTube_complaint_exhibits.pdf> Accessed 09 Jul., 2021.

[569]FEDERAL TRADE COMMISSION. **YouTube Complaint for Permanent Injunction.** Available at: <https://www.ftc.gov/system/files/documents/cases/ YouTube_complaint.pdf>, item 15. Accessed 09 Jul., 2021.

On September 4, 2019, it was announced[570] that Google[571] agreed to pay the $170 million arbitrated fine ($136 million to the U.S. Treasury and $34 million to the state of New York)[572].

Other mechanisms of action, in addition to the payment of fines, were also used by the agency in the agreement, such as prohibiting YouTube from continuing to collect personal information from children without parental consent, requiring the company to develop, implement and maintain a system for channel owners to determine whether their content is directed to the child, and also prohibit the platform and creators from using personal information that has already been collected[573].

The complaint listed several examples of platform channels, clearly aimed at children, who used target ads or behavioral advertising. That is, advertising based on data collection to create a specific behavior profile and subsequent delivery of targeted and individualized advertising.

Despite being categorized by age on the platform, the channels did not have any age adequacy requirement, nor did they require parental consent prior to collection through algorithms and cookies.

As of January 2020, videos aimed at children were limited in their features: comments; likes; live chat; stories; community guide; notification; viewers' ability to save videos, “watch them later”, or “save to a playlist” have been removed. The changes concern the video and not the viewer. This way, even adults can't comment,

---

[570]FEDERAL TRADE COMMISSION. **FTC Press Conference on Settlement With Google/YouTube**. Available at: <https://www.ftc.gov/news-events/audio-video/video/ftc-press-conference-settlement-google-YouTube> Accessed 09 Jul., 2021.

[571] The company Google owns the subsidiary YouTube through its parent company, Alphabet Inc..

[572]FEDERAL TRADE COMMISSION. 2021Order for **Permanent Injunction and Civil Penalty Judgment,** Fed. Trade Comm'n v. Google, LLC, No. 1:19-cv-2642. Available at: <https://www.ftc.gov/system/files/documents/cases/172_3083_YouTube_coppa_consent_order.pdf>. Accessed 09 Jul., 2021.

[573] FEDERAL TRADE COMMISSION. 2021Order for **Permanent Injunction and Civil Penalty Judgment,** Fed. Trade Comm'n v. Google, LLC, No. 1:19-cv-2642, p.10-12. Available at: <https://www.ftc.gov/system/files/documents/cases/172_3083_YouTube_coppa_consent_order.pdf> Accessed 09 Jul., 2021.

like, or access notifications of content targeted at children[574].

Since then, YouTube has a specific policy for the processing of children's data that extends internationally, including to Brazil.

The videos have lost, from the new *rule, the "target ads*", but not the contextual advertising, being those directed by the content of the video and not by the individualized profile of those who are watching it. Thus, the advertiser continues to be able to insert a toy advertising in a video aimed at the child, because he understands that that content matches the profile he seeks, without, however, having specificity of who is watching it and his individual preferences.

In this new approach, some channels have been impacted directly on their monetization[575], since personalized – and more profitable – ads are no longer displayed[576]. In an unofficial experiment, when disabling the possibility of "interest-based ads", i.e. target ads, the videos showed a loss of revenue between 60% and 90%[577].

Another possibility is that large advertisers look for already consolidated channels to have greater return on investment security. Previously, the criteria for sending advertising were by the user who was watching (target ads)*, and* not by the channel on which it was (contextual ads), as highlighted. That is, the interpretation of the best advertisement is made from the information collected from the producer of the video and its content and not from the end user, in this case, the child.

Although the platform makes use of artificial intelligence to identify

---

[574]Youtube. **Children's content FAQs**. Available at: <https://support.google.com/ YouTube/answer/9684541?hl=en-BR&ref_topic=9689353#zippy=%2Cquais-resources-n%C3%A3o-est%C3%A3o-dispon%C3%ADveis-em-conte%C3%BAdo-para-crian%C3%A7as-by-that-these-features-were-removed> 09 July,2021.

[575]Youtube. **YouTube Help**: Set Your Channel or Video's Audience, GOOGLE. Available at: <https://support.google.com/ YouTube/answer/9527654> Accessed 09 Jul., 2021.

[576]KATZ; Fener. Is a YouTube COPPAcalypse Coming? FTC Rules Could Start Demonetizing Creators in 2020, **TUBEFILTER**. Nov. 5, 2019. Available at: <https://perma.cc/D6CL-WGQR> Accessed 09 Jul., 2021.

[577] KATZ; Fener. Is a YouTube COPPAcalypse Coming? FTC Rules Could Start Demonetizing Creators in 2020, **TUBEFILTER**. Nov. 5, 2019. Available at: <https://perma.cc/D6CL-WGQR> Accessed 09 Jul., 2021.

audience targeting, content creators have been given the responsibility to self-state when, and if, the video is directed to children.

This was the first case that the FTC opened against a platform, covering responsibility for the content generated by its users. Not limiting, however, the possibility of investigating or prosecuting individual content creations for infringements of the agreement.

This point has raised many doubts as to the implementation of the agreement in practice. Creators had uncertainties when the content was childish, or mixed, for example.

However, since July of the same year, the agency had opened a public consultation for comments on the implementation of COPPA. Among them, item 25 questioned whether, in case of mixed audience, the hearing should be considered as childish, and therefore, strictly follow the rules imposed, or, in this case, be relaxed[578].

Questions derived from this extended to the presumption or not that there is a child audience watching children's content, implying a total ban, including for adults. On the other hand, risks were also considered by allowing general public sites to refute the presumption that all users of child-directed content are children[579].

The response would substantially change the impact of the agreement for both the platform and its users. So, Google responded the Public Request[580], as well as politicians, lawyers, industrial and commercial associations, YouTubers (and their

---

[578] FEDERAL TRADE COMMISSION. **Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842, 35843-44**. Available at: <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online> Accessed 06 Aug., 2021.

[579] FEDERAL TRADE COMMISSION. **Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842, 35843-44**, 25-e. Available at: <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online> Accessed 06 Aug., 2021.

[580] YOUTUBE. **Our comment on COPPA**. Dec.09.2019. Available at: <https://blog.YouTube/news-and-events/our-comment-on-coppa/> Accessed 06 Ago., 2021.

army of fans), among others, which generated almost 175,000 comments in general, by the deadline of December 11, 2019.

The day before the deadline, YouTuber "*KreekCraft*", with nearly 3 million subscribers to its channel on the platform, was received in Washington by the team coordinating the implementation of COPPA[581].

In conclusion, it was understood that, if they maintained the edges, it would not be possible to create by the platform, any type of content for children, which was not, in fact, the purpose of the law, which aims at the safety of children and their well-being and not their removal from the technological envelope which are already submerged.

Thus, from the dialogue between the parties, there was a better understanding of how the application of the standard should be. The interpretation of "directed to children" was made more flexible for mixed content, not considering, therefore, the presumption of child audience.

If a content, for example, has a familiar focus, but is not directly brought to minors, it can be considered a "general audience" and will not be impacted by the changes.

The self-declaration that the content is for children or not, follows parameters imposed by the FTC and updated by it as needed, on its website. It is understood that the decision should be based on the inclusion of actors, characters, activities, games, music or stories with content intended for children.

There is criticism in the terms of agreement, since the arbitrated value of the fine, since Alphabet Inc. (Google's parent company – responsible for YouTube) in 2018, amassed $136.819 billion in revenue and its net profit was $30.736 billion - up from $12.662 billion in 2017. Most of this being with advertising.

---

[581] KREEKCRAFT. **Youtube is saved**: coppa good news. YouTube FTC COPPA Update. Available at <https://www.youtube.com/watch?v=Ah5O5GeVjm4> Accessed 10 Oct., 2022.

It also added to the fact that the agreement avoided a lawsuit, in which, possibly, there would be a sentence condemning the company, with consequences to its market value. On the contrary, in the period of the agreement the company's shares rose[582].

Since it was an agreement, the company did not have to admit or deny the accusations of profit from illegal collection and used it to reposition itself in the market in favor of data protection.

Other criticisms go back to the fact that fundamental issues have not been in fact deepened and that children's data are still vulnerable. For example, the metrics used by the algorithms were not, and are still unclear. And even though the data, in general, is no longer collected, the necessary ones for the operations process are. However, it remains unclear what they refer to as necessary[583].

However, this is an example of great importance because it is currently the most accessed application by children, both in Brazil[584] and in the United States[585].

The FTC may also, in practice, charge any applications or websites that it believes are not complying with the law, even if based outside the United States, but which in turn are dealing with data from U.S. children. That's what happened in 2019

---

[582]Both the Class A and Class C stock rose in value steadily throughout September, 145 closing on September 30, 2019, with values of $1221.14 per share and $1219 per share, respectively. While stock markets are volatile, reflecting a seemingly endless number of factors, it is plausible that if the public perceives the settlement to be negative, Google's stock price would have fallen. O'DONNELL. Why the VPPA and COPPA Are Outdated: how Netflix, YouTube, and Disney+ can monitor your family at real cost. **Georgia Law Review**, vol. 55, no. 1, Fall 2020, p. 490.

[583]FERREIRA, Michelly Rosa; AGANTE, Luisa. The Use of Algorithms to Target Children while Advertising on YouTube Kids Platform: A reflection and analysis of the existing regulation. **International Journal of Marketing**, **Communication and New Midia, Special Issue 8** - Social Media Marketing, May 2020, p. 29-53.

[584]As for the use of applications by age. YouTube Kids: 0-3 years old 69%, 4-6 years old 71%, 7-9 years old 55% and 10-12 years old 34%. YouTube 0-3 years old 59%, 4-6 years old 63%, 7-9 years old 77% and 10-12 years old; 82% children access the app. PANORAMA MOBILE TIME/OPINION BOX. **Children and smartphones in Brazil.** October 2019. Available at: <https://www.mobiletime.com.br/pesquisas/criancas-e-smartphones-no-brasil-outubro-de-2019/> Accessed 29 Jun., 2021.

[585]Among the evidence presented in the lawsuit, the FTC used presentations by Google executives to toy industry customers in which YouTube is considered the "number 1 website regularly visited by children." Available at <https://www.ftc.gov/system/files/documents/cases/YouTube_complaint_exhibits.pdf> Accessed Jun 29, 2021.

with the Chinese app TikTok[586].

The FTC claimed that the company illegally collected personal data from children. The agency's reasoning was based, again, on the lack of permission of parents for their children to register on the site.

TikTok was sentenced to a $5.7 million fine as it proved to be a non-compliance with COPPA. Because of this violation, even after the penalty, the Chinese company had to include the "children only" modality in its application, and delete all data collected from children under the age of 13.

Thus, the need for cross-border look, including new global actors in the dynamics of data protection and children's privacy, has become clear as a way to bring effectiveness in its implementation in Brazil based on protection standards.

In the following item will be deepened the need to apply these criteria in the implementation of data protection and children's privacy in Brazil, as well as, recognizing the gaps in the debate.

7.2 The protection of children's data for commercial purposes from transnational standards

During the four years of development of this dissertation, some gaps in relation to children's data protection have been understood.

There was, until then, little international literature, and almost no national, on the subject. Data protection was always addressed from the adult's perspective, including children's data, since the consent of parents or guardians would equate the characteristics of legality to the processing of adult data.

In 2021, however, UNICEF[587] produced a manifesto on child data

---

[586] FEDERAL TRADE COMMISSION. **U.S. v. MUSICAL.LY.** Case 2:19-cv-01439. Available at: <https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc> Accessed 29 Jun., 2021.

[587] UNITED NATIONS CHILDREN'S FUND (UNICEF). **The Case for Better Governance of Children's Data**: a Manifesto. May 2021, p. 52 Available at:

governance in which it points out prerequisites necessary for their data protection: robust standards; implementation and lack of surveillance.

The manifesto comprises ten actions that challenge prevailing approaches to children's data[588]:

> 1. PROTECT children and their rights through child-centred data governance; 2. PRIORITIZE children's best interests in all decisions about children's data; 3. CONSIDER children's unique identities, evolving capacities and circumstances in data governance frameworks; 4. SHIFT responsibility for data protection from children to companies and governments; 5. COLLABORATE with children and their communities in policy building and management of their data; 6. REPRESENT children's interests within administrative and judicial processes, as well as redress mechanisms; 7. PROVIDE adequate resources to implement child-inclusive data governance frameworks; 8. USE policy innovation in data governance to solve complex problems and accelerate results for children; 9. BRIDGE knowledge gaps in the realm of data governance for children; 10. STRENGTHEN international collaboration for children's data governance and promote knowledge and policy transfer among countries.

Not all the items will be structured as an interpretative standard for the legal system in relation to the processing of children's data, since the dissertation is concerned about Brazilian legal system and its interpretation based on the best interest of the child from the gaps found in this.

However, it is possible to find similarities in the approach, which confirms, once again, that the protection of children's data only makes sense from a transnational understanding on the subject, given the convergences of protection systems that only take place if, in the end, they are in harmony.

In particular about the "bridge knowledge gaps" where the need to develop a "typology of harms" was pointed out, that could enable research and evidence about it. The dissertation brought this development in Chapter 2 in which it dealt with what is at risk in relation to data protection, and in Chapter 3 on the reasons why we must protect children's privacy.

<https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto> Accessed 05 Jul., 2021.

[588] UNITED NATIONS CHILDREN'S FUND (UNICEF). **The Case for Better Governance of Children's Data**: a Manifesto. May 2021. Available at: <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto> Accessed 05 Jul., 2021.

Other gaps are the need to better understand and defined the concept of “consent” and “the best interest of the child”, that is going to be explored in the following.

Thus, in understand the need for a transnational approach to data protection and the privacy of children, as well as existing gaps that could mitigate the effectiveness of protection, this sub-item aims to sustain a standard of data protection and privacy of children in Brazil, for commercial use.

This standard serves as a basis for the interpretation and regulation of the rights of the child before the protection of their data in Brazil. It is therefore not a "hard" standard typically used within manufacturing industry, like ISO that gives certain parallels to the range of quality management in the private sectors.

However, in the same way that as company might be forced to register to ISO to comply with customers’ expectations to their level of quality, similarly an accreditation system can be developed for data protection.

Although there is no specific regulation for legal articles brought in the LGPD, or that there are interpretative gaps on the theme of data protection of children in Brazil, the topics present here can/should be considered by the private sector to maintain an adequate level of protection to be developed and implemented by companies.

Based on the study throughout the dissertation, six items were listed based on transnational data protection standards, considering: the scope of privacy protection (chapter 1); the risks involved in the lack of data protection (Chapter 2); the impacts of the protection and regulation of child advertising (Chapter 3); transnational principles (Chapter 4); data protection already existing in Brazil (chapter 5) and the United States (chapter 6).

However, every given interpretation will take place in the best interest of the child. And this, in turn, is a varied content criterion. It has been showing up since the Convention on the Rights of the Child[589], in the Federal Constitution[590], in the

---

[589] UNICEF. **Convenção sobre os Direitos da Criança.** Brasília: UNICEF, 1989. Available at:

Statute of the Child and Adolescent[591] and in the General Data Protection Act itself[592].

To think about data protection focused on the best interests of the child, is to understand that, for all decisions, whether in the governmental sphere or even in companies, the rights of children should be prioritized.

From collection to processing and storage practices. From design to disposal. The governance of data must be based on the highest transnational standards that minimize the use of surveillance and algorithms to trace profiles of child behavior, for all the reasons exposed in this work.

The fragility of the public in question places them especially vulnerable to predatory practices and the legal interpretation in relation to them should always be based on their best interests, and not on the interest of parents, or even commercial.

Thus, considering that inadequate data protection makes room for mass surveillance, the discrimination of the algorithm models, among other harmful uses (item 2.2); that the culture of surveillance threatens the autonomy, self-determination and security of children (item 3.1.2); that the regulation of advertising is inefficient in Brazil because of the parameters adopted for this (item 3.2); that children's data can be used to manipulate and influence their behavior through abusive advertising (item 3.3); that Brazilian legislation is open to interpretation and little specific on the theme of data protection of children (chapter 5) and the North American too focused on the consent of parents or guardians (chapter 6); as well as both do not account for the evolution of children and their experiences compatible with their ages; and that there are transnational principles that inspire and base the creation of data governance laws and standards (chapter 4); it is understood that the protection of children's data, in their best interests, should consider at least:

(i) children's right by design;

<https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Accessed 09 May, 2022.
[590] Art. 227, CF.
[591] Art. 4º, ECA.
[592] Art. 14, caput, LGPD.

(ii) different needs by age group;

(iii) identification of the user as a child;

(iv) reassessment of the theory of consent;

(v) prohibition of targeted ads or native advertising.

Which will each be specified in its own topics.

7.2.1 Children's right by design

The first point that deserves to be highlighted in the interpretation of the rules of data protection of children in the LGPD, is in relation to the non-conditioning of the provision of data for participation in games, applications or other activities, in addition to those strictly necessary for the activity[593].

It is worth highlighting case judged by the STJ[594] in which it mentions the principle of data minimization, to substantiate as an unfair and illegal clause provided for in a credit card service agreement that authorizes the contracting bank to share consumer data with financial entities, without being given the option to disagree with that sharing.

From this understanding, for the use of data with a different purpose there should be a specific consent option. Thus, the treatment would be in accordance with the legal basis of consent.

However, when it comes to children's data, specifically for entry into games, applications or other activities, the interpretation should be restrictive**,** as it should always be based on their best interest.

Thus, unlike what would happen to the adult public, in which the controller

---

[593] Art. 14 (...) § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

[594] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1348532**. Relator: Ministro Luis Felipe Salomão, j. 10.10.2017.

could guarantee, through consent, various purposes for the processing of the data; the best interest of the child is not compatible with this interpretation.

In relation to children's data, the purpose should be restricted to the minimum necessary data processing for the operationalization of access, respecting the principle of necessity.

This understanding of the best interest needs to emerge along with the architecture of the systems, so that it is ensured, from design, that commercial interests do not overlap with those of children. A think of "children's rights by design".

It emerges a proper grammar on "children's rights by design" and a greater interaction between legal norms and system architectures based on the best interests of children

That is, an adequate legal application in the architecture of systems in which everyone is aware of the need for the protection of the child, the responsibility of the processing of this data and the scope of the rights to privacy and data protection.

For, as highlighted by the Federal Constitution, in Article 227, it is the duty of the family, society and the State to guarantee the child, with absolute priority, their rights.

The article mentions

> the right to life, health, nourishment, education, leisure, professional training, culture, dignity, respect, freedom and family and community life, as well as to guard them from all forms of negligence, discrimination, exploitation, violence, cruelty, and oppression (free translation).

Although it does not expressly cite data protection, which was incorporated as an autonomous fundamental right by constitutional amendment in 2021 (Chapter 2, item 2.1.3), it should also be included in the list of Article 227, and in Article 4 of the ECA, as the Right of the Child, and the duty of the State, the family and society to ensure it.

Of course, the child holds all the fundamental rights of adults, and that the specific ones brought by special law only add up to those. However, highlighting data

protection puts it at a level of shared responsibility.

It is not only the parents responsible for ensuring the best interest of the child. Society in general, as well as the State, must ensure the means for this to happen.

And this will happen, too, from the protection of children's data.

7.2.2 Different needs by age group

The LGPD distinguishes between the requirements for the processing of data from children (up to twelve years of age incomplete) and adolescents (up to eighteen years incomplete).

As for adolescents, in addition to the treatment being carried out aiming at the "best interest", the information about it should be provided in a simple, clear and accessible way. However, direct consent is valid. Unlike children, whose legal basis is the processing of data is the consent of parents or guardians.

At this point, the law takes into account the physical-motor, perceptual, sensory, intellectual and mental characteristics of the user, which must be taken into account when informing the target audience about the treatment.

This possible difficulty that the child has in understanding the limits of the processing of his personal data is due to the natural lack of maturity of his age.

That is, it is recognized that children have unique identities, and the legal interpretation must take place in accordance with the involving capacities of the child.

When thinking of a "children's right by design", it is also necessary to classify which child it’s talking about, at least in relation to age-appropriate design.

A child of pre-literacy age will not be informed in the same way as a child in their early school years or in the pre-adolescence transition years.

In this sense, efforts are needed to ensure that the regulation of the law takes place from the target audience reached, not putting all children at the same level of development, and, therefore, of vulnerability to the processing of data.

The Information Commissioner's Office (ICO), of the UK, created a code of practice for online services and set parameters for "age appropriate design", based on research from the London School of Economics and other sources[595]. In this, the stages of development were classified as follows:

0-5 Pre-literate & early literacy: This item is divided from age 0- 3, in which any understanding and awareness of online risks that have children within this age range is very limited. And the age 3-5 when children start to be developing friendships, learning to follow clear and simple's rules and have limited capacity for self-control. That also means that children in this age are "unlikely to have the cognitive ability to understand of follow more nuanced rules or instructions, or to make anything but the simplest of decisions"[596].

In this case, since they are pre-literate, text-based information should be very limited use in communicating with them.

6-9 Core primary school years children, for it turns, are more likely to have their own devices and use it independently. Children in this age range often prefer online gaming and creative based activities, may be experimenting with social media use and are vulnerable to be "influenced by online vloggers, particularly those within a similar age range"[597].

They are also likely to be developing a basic understanding of privacy concepts and some of the online risks for it. "They are unlikely however to have a clear understanding of the many ways in which their personal data may be used or of any less direct or obvious risks that their online behavior may expose them to" [598]. It's

---

[595] INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

[596] INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

[597] INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

[598] INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice

a group especially susceptible to the pressure of fitting with their peer group. However, family still being the strongest influencer.

10-12 Transition years is probably where the use of devices is more intense and used also to explore and develop self-identity and relationships. The need to "fit in"" socially increases the susceptibility to peer pressure, branding and online “influencers”, as well as the risks involving to it. In this age, children are “moving towards more adult ways of thinking but may have limited capacity to think beyond immediate consequences, be particularly susceptible to reward based systems, and tend towards impulsive behaviors”[599].

Even if children in this age have a better understanding of how things work, they are unlikely to be aware of less obvious uses of their personal data.

It also ranked, although out of the scope of this research, teenagers 13-15 years old, as early teens and 16-17 years old as approaching adulthood.

With these ideas it is possible to conclude that not necessarily a smaller child will demand stronger measures of protection. On the contrary. Very young children may be more protected within their limitations and parental control than children in the transition to adolescence, for example.

In any case, when devising the design for children it is necessary to list the risks and ways to protect the target audience in question, as a way to comply with their right to data protection and privacy.

As seen in item itself (chapter 6), the FTC, through the 1998 report, explored different levels of protection with for different ages,

In recommending the creation of a specific child data protection law, the Federal Trade Commission, through the 1998 report, explored different levels of

---

for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

[599] INFORMATION COMMISSIONER’S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

protection for different ages[600]. Whatever, when enacting the law, it was confirmed that COPPA protects children up to 13 years of age without any variability of age restrictions.

That doesn't mean that these differences are not considered in the practical cases.

On the contrary, the interpretation, for example, that all security measures have been complied with, necessarily involves assessing the risks to which users have been subjected. It is therefore impossible to disregard who the user is and his/her age in this assessment.

However, having previous regulatory parameters for the treatment of data differentiated by age groups seems to be the most appropriate way to have legal certainty in relation to the subject and approach a more effective protection of children's users' data.

Another point to be taken into account is the age difference, 12 years in Brazilian legislation, and 13 in the North American legislation. The age difference can create a vacuum of protection for children of at least one year, in cross-border situations, as are, in fact, much of the data processing. Thus, when aiming at a wide protection of childhood, with the possibility of extraterritorial use in Brazil, applications, websites or analogs should consider the parameter of better protection, that is, 13 years.

For all this to be possible, however, it is necessary to identify the child as such, as will be seen below.

7.2.3 Identification of the user as a child

One of the main weaknesses of child protection on the Internet is related to the identification of the user as a child profile. While applications or websites limit

---

[600] LANDESBERG, Martha K., LEVIN, Toby Milgrom; CURTIN, Caroline G.; LEV, Ori., **Federal Trade Commission, Privacy Online**: a report to congress (1998), p. 42. Available at <https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf> Accessed 10 Ago., 2021.

access to those over the age of 13, ensuring that this information is true is a point to be debated.

There was an emblematic case that brought a lot of debate about the theme of the identification of the child user: the case of the girl Antonella and TikTok[601]. The Italian child, 10 years old, died after performing a challenge called "blackout challenge" in the Tiktok app. Antonella went to the bathroom of her residence, alone, taking her cell phone and tried not to breathe for as long as possible in a row, which led to a fainting spell, followed by a coma, and death.

The case had much repercussion in the Italian media, including inciting the first regulatory moves on the application by the Italian Data Protection Authority.

The "Garante per la Protezione dei Dati Personali", determined the immediate blocking of the use of user data of the application, "for which there is no absolute certainty of age and, consequently, compliance with the provisions related to the personal data guidelines" (free translation)[602].

So TikTok blocked all Italian users and asked them to re-indicate their date of birth before continuing to use the app. That way, as soon as a user who claims to be under 13 years of age is identified, their account is removed.

The blocking order was substantiated by Article 24(2) of the Charter of Fundamental Rights of the European Union, which states that "all acts relating to children, whether carried out by public entities or by private institutions, shall primarily take into account the best interests of the child"[603], as well as recital 38 of the

---

[601] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok, a rischio la privacy dei minori:** il Garante avvia il procedimento contro il social network Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923> UNITED NATIONS CHILDREN'S FUND (UNICEF). **The Case for Better Governance of Children's Data**: a Manifesto. May 2021, p. 52 Available at: <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto> Accessed 05 Jul., 2022.

[602] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Provvedimento del 22 gennaio 2021** [9524194]. Available at: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524194> Accessed 05 Jul., 2022.

[603] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok**: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco del social. Available at:

General Data Protection Regulation (GDPR), which ensures that "children deserve specific protection with respect to their personal data", considering that they may "be less aware of the risks, consequences and guarantees" in relation to the processing of such data.

Two situations are crucial and take different paths regarding civil liability for the use of the minor, who lies when informing the age, to access the application, website or content: when the child, alone, circumvents the age verification system; or, when parents authorize and consent as if they were adults.

Em relação a última hipótese, relacionando-a ao caso trazido, houve uma campanha da autoridade italiana intitulada “If he is not old enough, social networks can wait” (free translation)[604]. The goal is to encourage parents to exercise the role of active supervision, paying special attention to when children are asked to indicate their ages for access. Still, and perhaps more importantly, do not encourage or lie about their children's age so that they have access to content not yet appropriate.

In relation to the first hypothesis, in which the child alone manages to circumvent the age verification system, the Italian Authority also mentioned Article 25, §1, of the same regulation, which requires the controller to adopt appropriate technical and organizational measures to implement the principles of the protection of personal data.

Since the use of these solutions requires a balance between the need for accurate verifications and the right to data protection of children and adolescents, the company has undertaken to start a discussion on the use of artificial intelligence for age verification purposes[605].

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524224#english_version> Accessed 05 Jul., 2022.

[604] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Se non ha l’età, i social possono attendere:** o spot del Garante privacy e di Telefono Azzurro per sensibilizzare i genitori. Available at: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9537523> Accessed 05 Jul., 2022. Also in **Minori e social. La campagna informativa del Garante e di Telefono azzurro.** Available at: <https://www.YouTube.com/watch?v=9nckmslOaaU> Accessed 05 Jul., 2022.

[605] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok si adeguerà alle richieste del**

It was also found that the Italian child had ten profiles on Instagram and three Facebook accounts, applications that also maintain the minimum age rule of 13 years for use[606].

The example cited is just one of thousands of cases of children improperly using apps, games, or accessing content outside their age limit.

TikTok is in Italy, as it is in Brazil, the United States and other countries of the European Union, exposing children of different nationalities and subjected to different legal regimes to the same service and the same conditions of use.

It doesn't matter if the challenge that led to the child's death was initiated here or there. Children need protection and this protection cannot find legal frontier to be consolidated.

Thus, it is suggested that, in relation to the indication of the child user, it is essential to: (i) those who process the data need to use all reasonable technical means to verify the validity of the information relating to the user's age; (ii) those who process the data need to indicate precisely how the age check adopted works to verify compliance with the minimum age group of registration (iii) those who process the data need to ensure access and correction of information by parents or guardians, or to do so on their own when verifying the inadequacy and (iv) those who treats the data needs to ensure the best interest of the child in the interpretation of mixed-audiences.

7.2.3.1 Those who process the data need to use all reasonable technical means to verify the validity of the information relating to the user's age.

Garante privacy. Ma l'Autorità vigilerà sull'effettiva efficacia delle misure che verranno adottate Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424> Accessed 05 Jul., 2022.

606 GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Minori sui social:** il Garante privacy apre fascicolo su Facebook and Instagram. La verifica sarà estesa anche agli altri social. Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9527301> Accessed 05 Jul., 2022.

The data operator shall implement technical solutions, within reasonable efforts, with the aim of ensuring that the information provided about age is true.

The idea of reasonable effort individualizes the technical ability of each operator to make this check. The techniques may be like those of consent validation.

Or, going further, as a cutting-edge solution, through "affective computing", brought in the work of Rosalind Picard[607], which proposes that computers must be able to learn emotions to act at the service of the human being.

Thus, it demonstrates possible models for the construction of computers capable of understanding and demonstrating affection, evaluating the emotions of individuals, their "automated emotional states".

The recognition of emotions can occur in the screening of emotional features (expressions, vocal intonation, gestures...), in different emotional episodes, along with physiological data collected by sensors. One more analysis should be made: about the environment and its characteristics that evoked an emotion. The following framework for computers to "have" emotions is suggested: emotional behavior; rapid primary emotions; cognitively generated emotions; emotional experience; mind/body interactions[608].

The approach presents the affective computing fusion model that processes both verbal and nonverbal information of users, making machines use this technology to predict when they are effectively treating children, or when they are trying to bypass the system by using it inappropriately.

Several research are being developed from affective computing.

> Affective Computing is a growing multidisciplinary field encompassing computer science, engineering, psychology, education, neuroscience, and many other disciplines. It explores how affective factors influence interactions between humans and technology, how affect sensing and affect generation techniques can inform our understanding of human affect, and on the design, implementation, and evaluation of systems that intricately involve

---

[607] PICARD, Rosalind Wright. **Affective computing**. Cambridge, MA: MIT Press.
[608] PICARD, Rosalind Wright. **Affective computing**. Cambridge, MA: MIT Press, 1997.

affect at their core[609].

This hypothesis approaches the dilemma of consent. If it is possible to understand that the consent of an adult was not free and voluntary, it is also plausible to identify when it is done by those who do not have the civil capacity to do so.

7.2.3.2 Those who process the data need to indicate precisely how the age check adopted works to verify compliance with the minimum age group of registration

This requirement depends on the principle of "transparency statement", that assumes that every data controller should give publicity in an accessible, clear, conspicuously, and accurately way of their activities.

In order to be properly monitored, it is necessary to be transparent with the information on how the age verification expressed by the user is made. Claiming that it is done by "reasonable technical means" is not enough. It is necessary to present them to justify their reasonableness.

7.2.3.3 Those who process the data need to ensure access and correction of information by parents or guardians, or to do so on their own when verifying the inadequacy

The principle of "access and correction" ensures that the data subject himself has access to what has been collected and that he/she can correct information he/she deems necessary. However, in the case of children's data - even if the operator is not at first unaware - so informed or asked by the parents must ensure access and correction to them.

Still, when realize a violation of use by a child, those who process the data should immediately proceed with the correction, and exclusion of the user. This whole process must, of course, be informed to the parents or guardians, whenever possible

---

[609] CALVO, Rafael Alejandro; D'MELLO, Sidney K., J. Gratch; KAPPAS, Arvid Kappas. **The Oxford Handbook of Affective Computing**. The Oxford University Press: 2014.

to contact them, to minimize possible damages caused to the minor.

Here, the identification of the child user is not confused with the validity of the consent supposedly given by the parents. This topic is restricted to when the application expressly limits the use for non-children and, therefore, consent passes through the assumption that one is a teenager or an adult making the decision.

7.2.3.4 Who treats the data needs to ensure the best interest of the child in the interpretation of mixed audiences

When the audience is multiple, that is, the target audience covers children and adults, for example, one should use the more restrictive interpretation of the rules. That is, treat mixed audiences as children's audiences.

As seen, in the YouTube case this was not the interpretation given. In this case, when the videos are classified as "family" the child's protection ends up being mitigated.

However, given the best interests of the child, whenever it is, even if not exclusively, the target audience of data processing, or, when there is knowledge of the use of the child user, good practices for the protection of children's data should be adopted.

So, publishers will need to identify and treat their adult and child audiences separately or adopt the most restrictive rules for both.

7.2.4 Reassessment of the theory of consent

Many doubts permeate the theory of consent in relation to fairness and validity, as already stated in chapter 2. On the other hand, both COPPA and the LGPD are based on consent about child data protection.

> What does consenting to something really mean? What should the law recognize as valid consent? Many transactions occur with some kind of inequality in knowledge and power. When are these asymmetries so substantial as to be coercive? The law's current view of consent is

> incoherent, and the law treats consent as a simple binary (that is, it either exists or it does not). Consent is far more nuanced, and privacy law needs a new approach that accounts for the nuances without getting too complex to be workable[610].

A theoretical legal standpoint would be to increase the mechanism of consent, to make it more elucidative, more informative, clearer and with more conscious decision-making.

The problem with this is that data protection standards are already focused on consent with too much appreciation of it. In this sense, "(…) strengthening consent mechanisms in law not only fails to take into account the reasonable interests of the party seeking consent, it also may end up further weakening the value of consent in practice"[611].

It will never be possible to be generally sure that every person behind consent has substantial knowledge of what is consented to. As well as do it freely. That is, consent, as already elaborated, is not synonymous with autonomy of will.

However valid and necessary attempts to make the terms of consent as clear, illustrated or as explicit as possible, yet it cannot be given the weight of being the absolute legal basis for parents' decisions regarding the data protection of their children.

Another theoretical legal standpoint would be denying consent and making data protection policies only informative about the practices provided for by law. That is, to restrict the possibility of data processing to what would be the "non-consent".

This alternative does not seem feasible in today's data economy. First because many people want to have the data collected – and it happens freely and clearly, for different reasons:

> (…) some people want targeted marketing. They want their data shared. They want catalogs to be mailed to their homes. They want to be tracked. They want to be profiled. They want companies to use their personal information to recommend products and services. These people should not

---

[610] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1899-1901.
[611] VAN DER HOF, Simone. Agree... Or do I?: a rights-based analysis of the law on children's consent in the digital world. **Wisconsin International Law Journal**, vol. 34, p. 101-136, 2016, p. 2.

> be dismissed as uninformed or foolish, as it is far from clear that the costs to these people outweigh the benefits[612].

Furthermore, the problem raised in Chapter 3 regarding the economic limits of restriction of data processing for commercial purposes is reached again. The collection, use and disclosure is what pays for the online content, as it is advertising what pays tv, radio and magazines content in general. The problem, of this bias, is that not necessarily people are fully aware that They are paying it with their personal data[613].

> Few engineers set out to build systems designed to crush privacy and autonomy, and few businesses or consumers would willingly use or purchase these systems if they understood the consequences. What happens more often is that the privacy implications of a new technology go unnoticed. Or if the privacy implications are considered, they are misunderstood. Or if they are understood correctly, errors are made in implementation. In practice, just a few mistakes can turn a system designed to protect personal information into one that destroys our secrets[614].

As problematic as the issue of consent is, it should not be abandoned. It is extremely relevant to give people a notice, access and the ability to control their data. While it is difficult to have the skills to make decisions that are always rational and informed, the alternative of not having any chance of a decision is much worse.

It is necessary, therefore, to reevaluate the theory of consent, its scope and interpretation in the practical application of the treatment of children's data in three aspects:

(i) Ensure efforts that improve self-management privacy through more consumer education, clearer notices, and ways to ensure that choices are as informed as possible.

This conduct also reflects on those who treat the data, since the practical effects of self-management have an impact not only on the data subject, “but in informing the companies that are collecting and using the data and in improving the

---

[612] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.
[613] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.
[614] TGARFINKEL, Simson. **The Death of Privacy in the 21st Century**. O'Reilly Media, 2008, p. 6.

companies' management of privacy"[615]. The process of creating privacy notices "forces internal changes within a company, raising self-awareness about data collection and use"[616].

(ii) Consent must be interpreted with all the nuances that may exist, in addition to the binary yes-or-no.

As seen, even for an adult the criteria are dubious. Parents are not expected to be data protection experts and always make sensible, free, and informed choices about the context in which they are consenting and their future implications for their children's lives. There are so many possibilities that it is impossible for an average adult to understand such a practical extension of the legal act in which he consents.

In relation to the child, even if doesn't participate of the consent, will need to deal with the consequences of the choices of the parents, or guardians, indefinitely. So on, (i.i) In the case of children's data, the best interest of the minor should overtake any autonomy of the parents' will in relation to possible interpretations of such consent. The alternative can be no other, but by the protection of the infant.

(iii) Furthermore, about the terms of privacy policies, these should be restricted to options already previously framed as appropriate to the child context, considering absolutely null and void the contrary[617].

Thus, it would be mitigating the autonomy of the will and giving greater regulatory control, in addition to the theory of consent, to the legality of the treatment of data of children.

It is giving consent the meaning it really has – of being a form of

---

[615] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1899-1901.
[616] SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1899-1901.
[617] In a manner analogous to the unfair terms of the Consumer Protection Code which are considered legally null and void in full.

expression of will not absolute, not always free and not always informed. Its validity should be conditioned to the concrete situation and absolutely restricted in relation to the consent given by parents in relation to children, always analyzing their best interest and other rights provided.

However, another problem brought by consent is to ensure its validity.

The first hypothesis is that the person responsible give consent in an invalid manner. Verification of the validity of such consent shall be checked on the condition of the operator of such data. However, artificial intelligence may be the cutting-edge criterion for extracting the motivations behind the choices.

These techniques are much studied and require greater theoretical deepening than is proposed in this short space within the work. However, it must be emphasized that the same technologies employed to build accurate profiles on users, it also can accurately determine whether children are under 13 (the minimum age many social media firms require their users to be).

The way this can be done, however, requires data collection, often sensitive, which should be avoided whenever another possibility exists, such as the use of biometrics and facial recognition.

> Emerging age estimation efforts broadly range from those based on biometric details, such as facial and hand analysis, to profiling people based on what they do and say. During the first three months of this year, TikTok removed 7 million accounts it suspected were created by under 13s; it previously said it uses facial recognition algorithms and people's connections to others to work out how old users may be. Facebook even uses, in part, the text in the "happy birthday" messages you receive[618].

The collection used in favor of child safety is plausible in data protection, but at the same time, "it would expand the amount of general surveillance technology

---

[618] BURGESS, Matt. This AI Predicts How Old Children Are: Can It Keep Them Safe? Yoti's tech may be enticing for Big Tech companies: It works out if you're under or over 13, the age most social media platforms require to create an account. **WIRED**. Available at: <https://www.wired.com/story/ai-predicts-how-old-children-are/> Accessed 17 Mar., 2022.

that children face on a daily basis"[619].

It is a dilemma that will need to be faced in an attempt to find new, safer and more balanced ways of recognizing the use of a child, in order to avoid exposure to inappropriate content, in balance with the least possible collection (minimization).

The interpretation of the technology available in favor of identifying the validity of consent should be a two-way route that recognizes the size of the responsibility for verifying validity from the scope of the specificities of the collection of information.

The more collections are made on the target audience, the greater the responsibility to identify their age.

Similarly, it happens in the second hypothesis, when consent is falsely given by children, posing as their parents. In this situation, verification of the validity of consent is presumably the responsibility of those who treat children's data.

The LGPD brought, in Article 14, Paragraph 5, that the controller must make all reasonable efforts to verify that consent has been given by the child's guardian, considering the available technologies.

The COPPA Rule says that an operator must choose a method reasonably designed considering available technology to ensure that the person giving the consent is the child's parent.

Neither COPPA nor LGPD mandate the method a company must use to get parental consent. The FTC, however, has determined that a number of consent methods meet that standard[620].

---

[619] BURGESS, Matt. This AI Predicts How Old Children Are: Can It Keep Them Safe? Yoti's tech may be enticing for Big Tech companies: It works out if you're under or over 13, the age most social media platforms require to create an account. **WIRED**. Available at: <https://www.wired.com/story/ai-predicts-how-old-children-are/> Accessed 17 Mar., 2022.

[620] FEDERAL TRADE COMMISSION. **Children's Online Privacy Protection Rule**: A Six-Step Compliance Plan for Your Business. Available at: <https://www.ftc.gov/business-

So**,** (iv) maintaining the issue of the validity of consent, as imposed by the LGPD and COPPA, but regulating the limits and methods of ensuring the desired standard**,** is another crucial point to the protection of children's data as well as their privacy.

Now, when falsehood is in the declaration of age – and then, in the ability to give consent or not, for applications that restrict use for over 13s, the issue of user identification as a child is entered, which was already addressed.

7.2.5 Prohibition of targeted ads or native advertising (merchandising)

The native adversiting, as called merchandising in Brazil, is a practice already regulated in the context of the Consumer Protection Code, by Resolution 163/2014 from CONANDA.

For, as already explained in topic 3.2, advertising should be recognized as advertising by the target audience to which it is intended to protect the consumer and make him aware that he is the recipient of a sponsored message that has commercial purposes, differing, for example, from journalistic content[621].

There is no doubt, in the legal interpretation, that it is, therefore, a sealed practice. However, as for behavioral targeting what one has are advertisements, clearly exposed as such, but that depend on a previously collected profile.

Under COPPA, GRPR or even LGDP, to process personal information from a child (other than in limited circumstances), it’s necessary to obtain verified parental consent before collection.

In practice, the search for consent in these situations is so difficult that the rule ends up prohibiting behavioral advertising, retargeting, or user profiling on most websites and apps that are directed to children.

---

guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4> Accessed 16 Mar., 2022.

[621] Art. 37, CDC.

This is not to say that all child advertising would be prohibited. But the use of advertising to child requires a strictly zero-data advertising technology to deliver it on a contextual basis only.

Therefore, it could be ensured that the collection of children's data always happens based on their best interest, respecting the transnational standards of protection, and closing the open interpretation given, currently, by the legislation in force in Brazil.

CONCLUSIONS

Considering the objective of the research presented in the Introduction of this paper: delimiting transnational standards of data protection of children in Brazil, the following hypotheses were raised:

a) The North American data protection model could be implemented in Brazil to broaden the interpretation of Article 14 of the General Data Protection Law;

b) Internal law rules, such as the Consumer Protection Code and the Statute of children and adolescents, would be enough for an extensive, sufficiently protective interpretation of children's rights to their data protection.

To confirm them, or not, the work was divided into seven chapters, each with a specific objective.

Chapter 1 analyzed the theoretical construction of the right to privacy and through a historical view of when and how the right to privacy emerged as a social, cultural, and legal idea, contextualizing it as a modern human right.

In the jurisprudential construction, from the U.S. Supreme Court, some cases were analyzed and had special relevance in the conception of the current application, as well as the interference of Brandeis, as judge of the Supreme Court and the author of a work of great influence on the subject.

Thus, it investigated in the doctrine the different attempts to conceptualize privacy, either as a single concept or as a multiple concept: the right to be left alone; limited access to the Self; secrecy; control over personal information; personhood and intimacy. This failure to find a concept of privacy presupposes the scope of the application of the theme, in addition to demonstrating that the right to data privacy is only one branch of the right to privacy.

Bert-Jaap Koops'[622] typology was then adopted, with a broad spectrum of

---

[622] KOOPS, Bert-Jaap; NEWEKKI, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom; GALIČ, Maša, A typology of privacy (March 24, 2016). **University of Pennsylvania Journal of**

application. It brought dimensions in eight different classifications of right to privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary and behavior), in addition to the ninth (informational) overlapping with the others.

Informational privacy, especially relevant to the study, is related to each of the other types as their non-physical manifestation. Thus, privacy not only protects the body, space, communications, or behaviors, but also directly protects information about them. Although, by protecting such information, it often enters the "physical" territory of protection.

This classification then approximates from data protection, treated in the next chapter.

Chapter 2, in turn, specified the right to data protection in its peculiarities, differentiating it from the right to privacy and data security and classifying as a fundamental autonomous right.

The chapter also highlighted what's at risk about data protection: the value of personal information; the discrimination of algorithm models; the guarantee of "free consent"; data breach and the false anonymization of information.

As well as pointed out the arguments against the data privacy protection popularly used, such as: the death of privacy; the I have nothing to hide argument; the privacy as opposed to the public interest and the false trade-off.

Ending the initial conceptualizations on the subject, it was necessary to enter the particularities of childhood as a group of special need for protection regarding their data.

Thus, Chapter 3 looked to understand the vulnerability of children to the media, especially the effects of surveillance in their autonomy, self-determination and security.

Using a social and legal approach, the chapter also addressed childhood and the special protection required of this category, as well as the regulation of

---

International Law 38(2), p. 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, p. 2. Available at: <https://ssrn.com/abstract=2754043> Accessed 25 Mar., 2018.

children's advertising in Brazil.

Two types of advertising were especially relevant in this analysis: the so-called target ads and the native advertising, known in Brazil as merchandising; for its evident abuse to children.

Nevertheless, companies based outside Brazil, as highlighted in this same item, maintain practices incompatible with the national legal system and rely on their own regulations to determine the limits of action.

For this reason, the next Chapter moved forward on the principles of data protection in a transnational view.

So on, Chapter 4 was dedicated to the transnational principles of data protection, collected from Schwartz and Solove's analysis of different regulatory bases around the world, to suggest a standard of protection to be considered for building standards or regulations in the United States.

The need for this chapter of the research is based on the perspective that these same transnational parameters were confronted with Brazilian standards and must also be observed in the adoption of criteria for the protection of child data, to reach a level of protection of transnational compliance.

The work advances to Chapter 5 that addressed the main elements of child data protection and privacy in Brazil.

Brought the regulatory frameworks as: purpose; adequacy; necessity; free access and data quality; transparency; security; liability and accountability; non-discrimination; prevention; portability; confidentiality; consent and onward transfer; relating them to the transnational principles set out in the previous chapter.

From a dialogued reading of the General Data Protection Law with other legal sources, such as the Federal Constitution, Consumer Protection Code and the Statute of Children and Adolescents, sought the idea of hypervulnerability and the protection against misleading and abusive advertising, coercive or unfair commercial methods and abusive practices or terms.

It also concluded with considerations about the National Data Protection Authority and the possible administrative sanctions that can be applied in specific

cases.

Chapter 6 sought the same elements in the United States, from the Children's Privacy Protection Act (COPPA), trying to identify convergences and divergences with Brazilian legislation.

The regulatory framework took place about: consent; information security; time and quality of information; on-conditioning of the service to information other than those necessary for the operation of the same and the Safe Harbor.

From dialogue with other internal sourcers, the California Consumer Privacy Act was considered, as well as the non-ratification of the United Nations Convention on the Rights of the Child and the reasons for it.

The chapter also addressed to the regulation of advertising for children and the role of Federal Trade Commission.

Finally, Chapter 7 pointed out the necessary transnational approach to the implementation of child data protection for commercial purposes, using the concept of Frydman[623] for "standards" as rules created by private institutions, devoid of political responsibility (accountability), and without state participation, which condition the behavior of the State and the individual, generating a real tension by the lack of sovereign acts in the participation of norms increasingly present in world society.

But going further, contemplating also the rules created by States when applied outside their jurisdiction. This is the obvious case of COPPA, which has become a standard because it has influence not only in the United States, but also in the creation and implementation of standards by other public and private entities around the world.

An emblematic example brought in this perspective was the case FTC versus YouTube. In addition to being the largest deal ever made by the Commission, the part (YouTube), is the second most visited site in the world and currently the most accessed by children both in Brazil and in the United States, as seen.

---

[623] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018.

The agreement between the Federal Trade Commission and YouTube is imposed as a **standard in the protection of transnational children's data**. The company, after signed the agreement, applied it outside the territoriality imposed by, probably as a marketing strategy to meet the highest requirements. It is not a necessarily state imposition, but an analysis of the "best quality" to be used in data protection actions, according to established standards.

As a consequence, it modified the way of processing data of millions of children worldwide, through the platform showing to be a "transnational standard" in relation to the theme.

As Frydman warned, "it is not necessary to treat the standard as a formal source of law, which it is not, but considers more, from a pragmatic point of view, the effects of regulation that it produces"[624].

It is not necessary to discuss the mandatory or coerciveness of a standard, when it, in fact, takes effect for reasons other than those of legal rules.

As in the agreement between the U.S. authority and YouTube, "the rule of law is shifted to some extent to the functions of justification of previous consensual decisions concluded in transnational scenarios" (free translation)[625].

On the other hand, until then the Brazilian national rules of advertising regulation were, and continue to be, ignored by YouTube in Brazil, as well as by other websites and applications that clearly provide advertising to children, even if not directed from the collection of data.

Domestic law is removed when it does not agree with the proposed standard. Proving, therefore, the empire of standards on the rule, in the specific case, brought by new global actors, which delimit, in practice, how the data of millions of children are treated.

---

[624] Benoit FRYDMANN**. The end of the rule of law**. Govern by standards and indicators. Translation of Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018, p. 83.

[625] STAFFEN, Márcio Ricardo. **Interfaces do Direito Global**. 2. ed. ampl. atual. Rio de Janeiro: Lumen Juris, 2018, p. 30

The coerciveness and legitimacy of the state normative source seem to have no practical importance when comparing the two situations: on the one hand the effectiveness without coercibility and legitimacy of an agreement from another nation, and on the other, and ineffectiveness with coercibility and legitimacy of a resolution based on Brazilian federal law.

In this sense, the protection of child data needs to be debated from the perspective that standards from different actors, as in the case of the Federal Trade Commission in its interpretation of the Children's Online Privacy Protection Act, which generate effects of regulation to domestic law, even if they are not a formal source.

Several criticisms can be formulated. As far as the case is concerned, the standards, as technical standards produced by different sources, legitimacy or coerciveness based on legal rules and are devoid of accountability. This is probably the reason that leads the company to disregard the prohibition of advertising to children in Brazil to the detriment of profit.

Finally, despite being devoid of political responsibility, they are not necessarily devoid of political interests. Technical standards are, finally, although based on the scientificity of the research, a choice of pattern that may have interferences of the most diverse, including political or economic ideologies.

Regardless of the criticisms, it is evident the plurality of state and transnational normative sources that merge in contemporary relations of power, since pragmatic point of view, the effects exist, as in the case analyzed.

As well as the asymmetry of forces between them. If, on the one hand, standards lack legitimacy or coerciveness, on the other hand, legal rules seem to suffer from the same problem in relation to global actors who refuse to subordinate national sovereignty.

The example of the YouTube case reveals, in practice, the diagnosis prescribed by Frydman pointing out the need to look beyond the classical sources of national or international law, and to return attention to new sources, such as the standards generated by new actors who dictate, in fact, the rules of the game.

Thus, considering that inadequate data protection makes room for mass surveillance, the discrimination of the algorithm models, among other harmful uses (item 2.2); that the culture of surveillance threatens the autonomy, self-determination and security of children (item 3.1.2); that the regulation of advertising is inefficient in Brazil because of the parameters adopted for this (item 3.2); that children's data can be used to manipulate and influence their behavior through abusive advertising (item 3.3); that Brazilian legislation is open to interpretation and little specific on the theme of data protection of children (chapter 5) and the North American too focused on the consent of parents or guardians (chapter 6); as well as both do not account for the evolution of children and their experiences compatible with their ages; and that there are transnational principles that inspire and base the creation of data governance laws and standards (chapter 4); it is understood that the protection of children's data, in their best interests, should consider at least:

- children's right by design;
- different needs by age group;
- identification of the user as a child;
- reassessment of the theory of consent;
- prohibition of targeted ads or native advertising.

Each one was individually explained in the last chapter in which it brings the originality of the thesis in pointing out the ways in which the interpretation of the best interest of the child should take place in relation to the protection of their data, in Brazil.

For all already considered, the first hypothesis has not been confirmed. COPPA alone could not sufficiently cover the interpretation given to the General Data Protection Act, in particular because it is too rely on consent. This theory should be reevaluated in its application to children, as suggested in chapter 7.

The second hypothesis, regarding the Brazilian internal rules being

sufficient for an extensive interpretation of the data protection of children in Brazil, was partially confirmed.

The Brazilian norm, because it is not yet regulated and is quite open to interpretations, could be extensively adapted to the themes proposed at the end of the last chapter. However, this reality cannot be evaluated at the moment, as it still lacks practical experience.

However, it is important to consider that protecting children's privacy means protecting the private space that is required for the construction of self. A sphere in which it makes that individual unique, with unique thoughts, feelings, and meanings.

Protect autonomy and freedom to explore the search for an identity without being exposed or watched by strangers. Or the opportunity for social engagement with free choices about what to share or what to keep private.

It also means a democratic value of self-determination. That is, to make r choices based on free conviction, and not by the media manipulation that has known that person since the first virtual steps, perhaps more intimately than their parents, or even perhaps themselves.

BIBLIOGRAPHY

AIKEN, Mary. **The Kids Who Lie About Their Age to Join Facebook**. The ATL. Available at: <https://www.theatlantic.com/technology/archive/2016/08/the-social-mediainvisibles/497729/> Accessed 09 Jul., 2021.

ALANA. Criança e Consumo. **15 empresas - Canais de YouTubers Mirins:** Publicidade na Internet (março/2016) Available at: <https://criancaeconsumo.org.br/acoes/YouTubers-mirins/> Accessed 18 Jul., 2022.

ALANA. Criança e Consumo. **9 empresas**: Publicidade infantil em canais de YouTubers Mirins (agosto/2021) Available at <https://criancaeconsumo.org.br/acoes/9-empresas-publicidade-infantil-em-canais-de-YouTubers-mirins-agosto-2021/> Accessed 18 Jul., 2022.

ALEXANDER, Christopher Bret. The General Data Protection Regulation and California Consumer Privacy Act: the economic impact and future of data privacy regulations, 32 **LOY. Consumer Rev.** 199. 2020.

ALLEN, Anita. **Uneasy Access**: privacy for Women in a Free Society. Rowman & Littlefield Publishers, 1988.

ALVAREZ, Daniel. **Safe Harbor is Dead**; long live the Privacy Shield? A.B.A., (May 20, 2016), Available at <https://www.americanbar.org/groups/business-law/publications/blt/2016/05/09_alv arez/> Accessed 04 Sept., 2021.

ALVES, Fabricio da Mota. Chapter VIII: surveillance in BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD**: General Data Protection Law Commented. Sao Paulo: Thomson Reuters Brazil, 2019, p. 268-369.

ANDREWS, Lori**. I Know Who You Are and I Saw What You Did**: Social Networks and the Death of Privacy. Free Press, 2012.

APEC – Privacy Framework (2005)

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. Ed. Rio de Janeiro: Forense Universitária, 2007.

ARISTÓTELES. **Política**. Tradução de Mário da Gama Kury, 3. Ed. Brasília: editora Universidade de Brasilia, 1997.

ATTIAH, Karen. Why won't the U.S. ratify the U.N.'s child rights treaty? **The Washington Post.** November 21, 2014 at 4:12 p.m. EST. Available at: https://www.washingtonpost.com/blogs/post-partisan/wp/2014/11/21/why-wont-the-u-s-ratify-the-u-n-s-child-rights-treaty/ Acess in 24 jul. 2022.

BARBARO, Michael; ZELLER, Tom. A Face Is Exposed for AOL Searcher No. 4417749,

BARBARO, Michael; ZELLER, Tom. A Face Is Exposed for AOL Searcher No. 4417749, **N.Y. TIMES**, Aug. 9, 2006, Available at: <https://www.nytimes.com/2006/08/09/technology/09aol.html> Accessed 13 Apr., 2020.

BBB National Programs. **Children's Advertising Review Unit (CARU).** Available at: <https://bbbprograms.org/programs/all-programs/children's-advertising-review-unit> Accessed 17 Jul., 2022.

BBB National Programs. **Children's Advertising Review Unit (CARU).** Self-Regulatory Guidelines for Children's Advertising. Available at: <https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/ default-source/caru/caru_advertisingguidelines.pdf> Accessed 17 Jul., 2022.

BENJAMIN, Antônio Herman V; MARQUES, Claudia Lima Marques; MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3. ed. São Paulo: Thomson Reuters Brasil, 2019. E-book.

BENJAMIN, Antônio Herman Vasconcellos; BESSA, Leonardo Roscoe; MARQUES, Cláudia Lima. **Manual de direito do consumidor**. 5. ed., ver., atual. e ampl. São Paulo: Revista dos Tribunais, 2013, p. 47.

BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988.

BENNET, Colin; RAAB, Charles. **The Governance of Privacy**: Policy Instruments in the Digital Age, MIT University Press, 2006.

BENNETT, Colin. Convergence Revisited: Toward a Global Policy for the Protection of Personal Data. **Technology and Privacy**: the new landscape. January 1997. Cambridge: MIT Press, p. 113.

BENNETT, Colin. **Regulating privacy**: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press, 1992.

BENNETT, Collin. J. LYON, David. **Data-driven elections**: implications and challenges for democratic societies. Internet Policy Review, 8(4) 2019. Available at: <https://doi.org/10.14763/2019.4.1433> Accessed 25 Jul., 2022.

BENTHAM, Jeremy. **The panopticon**: or the inspection house. London: mews-gate, 1787.

BERTRAND, André. **Droit à la vie privée et droit à l'image**. Paris: Litec, 1999.

BIG THINK. **Judge Richard Posner:** privacy. Available at <https://www.YouTube.com/watch?v=kQu0et1jXfs> Accessed 26 Jan., 2021.

BINNIG, Christian F.; COMSTOCK, Christopher S., The California Consumer Privacy Act: the first step towards an american GDPR, **Infrastructure**, vol. 58, n. 4, summer 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 46.

BIONI, Bruno Ricardo. **Protection of personal data**: the function and limits of consent. Rio de Janeiro: Forensics, 2019, p. 175-176.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019.

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD**: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019.

BOK, Sissela. **Secrets**: On the Ethics of Concealment and Revelation 10-11 (1983).

BRITANNICA. **Algorithm**. Available at <https://www.britannica.com/science/algorithm> Accessed 03 Set., 2021.

BURGESS, Matt. This AI Predicts How Old Children Are: Can It Keep Them Safe? Yoti's tech may be enticing for Big Tech companies: It works out if you're under or over 13, the age most social media platforms require to create an account. **WIRED**. Available at: <https://www.wired.com/story/ai-predicts-how-old-children-are/> Accessed 17 Mar., 2022.

BYRNE, J., KARDEFELT-WINTHER, D., LIVINGSTONE, S., & Stoilova, M. (2016). **Global Kids Online Research Synthesis** (2015-2016). UNICEF Office of Research – Innocenti and London School of Economics and Political Science. Available at: <http://globalkidsonline.net/wp-content/uploads/2016/11/Synthesisreport_07-Nov-2016.pdf> Accessed 08 Jan., 2021.

CALVO, Rafael Alejandro; D'MELLO, Sidney K., J. Gratch; KAPPAS, Arvid Kappas. **The Oxford Handbook of Affective Computing**. The Oxford University Press: 2014.

CASSESE, Sabino. **Chi governa il mondo?** Bologna: Il Mulino, 2013.

CASTELLS, Manuel. **Rise of the newwork society**: the information age: economy, society and culture. Vol. I, second ed. 2009.

CENTER FOR MEDIA EDUCATION (CME), **Web of Deception**: Threats to Children From Online Marketing (1996). Available at: <http://www.cme.org/children/marketing/deception.pdf> Accessed 04 May., 2022.

COHAN, Peter. Four Reasons Google Bought Waze. **Forbes**. Available at: <https://www.forbes.com/sites/petercohan/2013/06/11/four-reasons-for-google-to-buy-waze/?sh=1109838f726f> Accessed 08 Set., 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. (2020). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: **TIC Kids Online Brasil 2019**. São Paulo: CGI.br. Available at: <https://cetic.br/media/docs/publicacoes/2/20201123093344/tic_kids_online_2019_liv

ro_eletronico.pdf> Accessed 27 May, 2019.

CONNOLLY, Chris. **The US Safe Harbor**: fact or fiction? 1, 4, 7 (2008), Available at <http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf> Accessed 04 Sept., 2021.

CONSELHO NACIONAL DE AUTO-REGULAMENTAÇÃO PUBLICITÁRIA – CONAR. **Código Brasileiro de Auto-regulamentação publicitária**. Available at: <http://www.conar.org.br/codigo/codigo.php> Accessed 18 Jul., 2022.

COOLEY, Thomas. **A treatise of the law of torts**: or the Wrongs which Arise Independent of Contract. Callaghan: Michigan University, 1879. 775 p.

CRIANÇA E CONSUMO. **Mattel**: você YouTuber escola Monster High (fevereiro/2017). Available at: <https://criancaeconsumo.org.br/acoes/mattel-do-brasil-ltda-voce-YouTuber-escola-monster-high-fevereiro2017/> Accessed 08 Aug., 2022.

CURY, Munir (coord.). **Estatuto da criança e do adolescente comentado**: comentários jurídicos e sociais. 9ª ed., atual. São Paulo: Malheiros, 2008, p. 36

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

DOUGHERTY, Christie, Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU E-Privacy Regulation, 12 **NE. U. L. REV**. 629, 658 (2020).

EDWARDS, Lilian; HATCHER, Jordan. Consumer privacy law 2: data collection, profiling and targeting. In: EDWARDS, Lilian; WAELDE, Charlotte (Coord.). **Law and the internet**. Portland: Har Publishing, 2009. p. 516-517

ELECTRONIC PRIVACY INFORMATION CENTER. **The Administrative Procedure Act (APA).** Available at: <https://www.justice.gov/sites/default/files/jmd/legacy/2014/05/01/act-pl79-404.pdf> Accessed 09 Jul., 2021.

ELLIOTT, Margaret S. Examining the Sucess of computerization movements in the ubiquitous computing era: free and opensource software movements in LLIOTT, Margaret S.; KRAEMER, Kenneth L. Computerization movements and technology diffusion: from mainframes to ubiquitous computing. **INFORMATION TODAY**, Inc: Medford: New Jersey, p. 351.

FEDERAL COMMUNICATION COMMISSION. **Children's Educational Television.** Available at: <https://www.fcc.gov/consumers/guides/childrens-educational-television> Accessed 18 Jul., 2022.

FEDERAL SENATE. **Provisional measure No. 869** of 27 December 2018. Amends Law No. 13,709 of August 14, 2018, to provide for the protection of personal data and

to create the National Data Protection Authority and provides other measures. Available at <https://legis.senado.leg.br/norma/30762959/publicacao/30762970> Accessed 28 Jun., 2022.

FEDERAL TRADE COMISSION. **Google LLC and YouTube, LLC.** Available at: <https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-YouTube-llc> Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. 16th CFR Part 312. **Children's Online Privacy Protection Rule**: final rule. 59888 Federal Register / Vol. 64, No. 212 /Wednesday, November 3, 1999 /Rules and Regulations. Available in: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/childrens-online-privacy-protection-rule-16-cfr-part-312/991103childrensonlineprivacy.pdf. Accessed 28 Jun., 2021.

FEDERAL TRADE COMMISSION. 2021Order for **Permanent Injunction and Civil Penalty Judgment,** Fed. Trade Comm'n v. Google, LLC, No. 1:19-cv-2642. Available at: <https://www.ftc.gov/system/files/documents/cases/172_3083_YouTube_coppa_consent_order.pdf>. Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. **A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority**. July 2018. Available at: <https://www.ftc.gov/about-ftc/mission/enforcement-authority> Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. **Children’s Online Privacy Protection Rule**: A Six-Step Compliance Plan for Your Business. Available at: <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4> Accessed 16 Mar., 2022.

FEDERAL TRADE COMMISSION. **Complaint Exhibits A - C**. Case 1:19-cv-02642 Document 1-1 Filed 09/04/19. Available at: <https://www.ftc.gov/system/files/documents/cases/YouTube_complaint_exhibits.pdf> Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions, FED. TRADE COMM'N § B(3) (July 2020), Available at: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>. Accessed 04 May, 2022.

FEDERAL TRADE COMMISSION. **Complying with COPPA**: Frequently Asked Questions. Available at: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. **FTC Press Conference on Settlement With Google / YouTube.** Available at: <https://www.ftc.gov/news-events/audio-

video/video/ftc-press-conference-settlement-google-YouTube> Accessed 09 Jul., 2021.

Federal Trade Commission. **Internet Cookies**. Available at: <https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies> Accessed 04 May, 2022.

FEDERAL TRADE COMMISSION. **Legal Library:** Cases and Proceedings. Available at: <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3002-unixiz-inc-doing-business-i-dressupcom> Accessed 04 May, 2022.

FEDERAL TRADE COMMISSION. **Privacy Online**: A Report to Congress. Available at: <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (June 1998). Accessed 4 May, 2022.

FEDERAL TRADE COMMISSION. **Privacy Online**: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000). Available at: <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> Accessed 4 May, 2022.

FEDERAL TRADE COMMISSION. **Privacy Online**: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000), Available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> Accessed 04 May, 2022.

FEDERAL TRADE COMMISSION. **Protecting Consumer Privacy in an Era of Rapid Chang**e: Recommendations For Businesses and Policymakers. March, 2012. Available at: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers> Accessed 03 Mar., 2021.

FEDERAL TRADE COMMISSION. **Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842, 35843-44**. Available at: <https://www.federalregister.gov/documents/2019/07/25/2019-15754/request-for-public-comment-on-the-federal-trade-commissions-implementation-of-the-childrens-online> Accessed 06 Ago., 2021.

FEDERAL TRADE COMMISSION. **Statement of Basis and Purpose on Children's Online Privacy Protection Rule Final Rule**, 78 Fed. Reg. No. 12 3972-2996 (Jan. 17, 2013). Available at: <https://www.ftc.gov/system/files/2012-31341.pdf> Accessed 09 Jul., 2021.

FEDERAL TRADE COMMISSION. **U.S. v. MUSICAL.LY.** Case 2:19-cv-01439. Available at: <https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc> Accessed 29 Jun., 2021.

FEDERAL TRADE COMMISSION. **YouTube Complaint for Permanent Injunction.** Available at: <https://www.ftc.gov/system/files/documents/cases/YouTube_complaint.pdf>, item 15. Accessed 09 Jul., 2021.

FERREIRA, Michelly Rosa; AGANTE, Luísa. The Use of Algorithms to Target

Children while Advertising on YouTube Kids Platform: A reflection and analysis of the existing regulation. **International Journal of Marketing**, **Communication and New Midia, Special Issue 8** - Social Media Marketing, may 2020.

FERRER, G. R. Soberanía y transnacionalidad: antagonismos y consecuencias. Barcelona - Revista de Derecho - España. **Revista de Derecho vLex**, v. 63, p. 1-., 2008.

FLAHERTY, David H. **Protecting Privacy in Surveillance Societies**: The Federal Republic of Germany, Sweden, France, Canada, and the United States. The University of North Carolina Press, 1992.

FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. New York: Oxford University press, 2014.

FOULCAULT. Michel. **Discipline and punish**. New York: vintage, 1995. Surveiller et Pnir: Naissance de la prison. Paris: Gallimard, 1975..

FREEMAN, Wilson C. California Dreamin' of Privacy Regulation: the California consumer privacy Act and congress. **Congressional Research Service**, 2018.

FRYDMANN Benoit**. O fim do Estado de Direito**. Governar por standards e indicadores. Tradução de Jânia Saldanha. Porto Alegre: Livraria do Advogado, 2018.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Minori e social. La campagna informativa del Garante e di Telefono azzurro.** Available at: <https://www.YouTube.com/watch?v=9nckmslOaaU> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Minori sui social:** il Garante privacy apre fascicolo su Facebook e Instagram. La verifica sarà estesa anche agli altri social. Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9527301> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Provvedimento del 22 gennaio 2021** [9524194]. Available at: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524194> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Se non ha l'età, i social possono attendere:** o spot del Garante privacy e di Telefono Azzurro per sensibilizzare i genitori. Available at: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9537523> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok si adeguerà alle richieste del Garante privacy**. Ma l'Autorità vigilerà sull'effettiva efficacia delle misure che verranno adottate Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok, a rischio la**

privacy dei minori: il Garante avvia il procedimento contro il social network Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923> Accessed 05 Jul., 2022.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. **Tik Tok**: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco del social. Available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524224#english_version> Accessed 05 Jul., 2022.

GARFINKER, Simson. Database Nation: **The Death of Privacy in the 21st Century**. O'Reilly Media, 2001.

GAVISON, Ruth. Privacy and the limits of law. **The Yale Law Journal,** vol. 89, n. 3 (Jan., 1980) p. 421-471, p. 438. Available at <http://www.jstor.org/stable/795891> Accessed 10 Aug., 2018.

GINDIN, Susan E., Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 **SAN DIEGO L. REV.** 1153, 1170 (1997).

GODKIN, L., E.L. Libel and Its Legal Remedy. **12 Journal of Social Science** 69, 80 (1880).

GOOGLE, CONAR. **Guia de boas práticas para a publicidade online voltada ao público infantil.** Available at <http://www.conar.org.br/pdf/guia-infantil-conar.pdf> Accessed 08 Aug., 2022.

GRAHAM SCOTT, Gini. **The Death of Privacy**: The Battle for Personal Privacy in the Courts, the Media, and Society. Changemakers Publishing, 2015.

GROSS, Hyman. The Concept of Privacy. **43 New York University Law Review** 34, 35-36 (1967)

HAAG, Ernest Van Den. On Privacy in **Nomos XIII**: Privacy 149, 149 (J. Roland Pennock & J. W. Chapman eds., 1971).

HABERMAS, Jürgen. **Mudança estrutural da esfera pública**: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014, p. 97-98.

HERMAN BENJAMIN, Antonio. **Código Brasileiro de Defesa do Consumidor**, 6ª edição, Editora Forense Universitária, 1999.

HERTZEL, Dorothy A. **Don't Talk to Strangers**: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online, 52 FED. COMM. L.J. 429, 431 (2000).

IAPP. **Global Privacy Law and DPA Directory.** Available at: <https://iapp.org/resources/global-privacy-directory/> Accessed 01 Mar., 2022.

IAPP. **Global Privacy Law and DPA Directory**. Available at:

<https://iapp.org/resources/global-privacy-directory/> Accessed 01 Mar., 2022.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Age appropriate design**: a code of practice for online services. Annex B: age and development stages. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/> Accessed 28 Sep., 2022.

INNESS, Julie. **Privacy, Intimacy, and Isolation**. New York and Oxford: Oxford University Press, 1992, p. 6.

INSTITUTO ALANA. Criança e Consumo. **Normas em vigor**. Lei nº: 8.078/1990 – Código de Defesa do Consumidor (CDC) comentado. Available at: <https://criancaeconsumo.org.br/normas-em-vigor/codigo-de-defesa-do-consumidor-cdc-comentado/> Accessed 18 Jul., 2022.

INSTITUTO ALANA. Criança e consumo. **Publicidade infantil é ilegal**: entenda o impacto da Resolução 163/2014 do Conanda. Available at: <https://criancaeconsumo.org.br/wp-content/uploads/2014/02/Publicidade-Infantil-%C3%A9-ilegal.pdf> Accessed 05 Sep., 2022.

INTERACTIVE ADVERTISING BUREAU. **Guide to navigating COPPA**: recommendations for compliance in an increasingly regulated children's media environment. October 2019, p. 7. Available at: <https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf> Accessed 17 Jul., 2022.

INTERNET MANAGEMENT COMMITTEE IN BRAZIL - CGI.br. **Research on the use of the Internet by children and adolescents in Brazil**: TIC kids online Brazil 2017. Survey on internet use by children in Brazil: ICT kids online Brazil 2017 [e-book] / Núcleo de Informação e Coordenação do Ponto BR, [editor]. -- São Paulo: Internet Steering Committee in Brazil, 2018. Available at: <https://cetic.br/media/docs/publicacoes/2/tic_kids_online_2017_livro_eletronico.pdf> Accessed 01/04/2019.

JANGER, Edward. Locating the Regulation of Data Privacy and Data Security. **Brooklyn Journal of Corporate, Financial & Commercial Law**, vol. 5, no. 1, Fall 2010, p. 97-110. HeinOnline, p. 99.

JARGAN, Julie. How 13 Became the Internet's Age of Adulthood: The inside story of COPPA, a law from the early days of e-commerce that is shaping a generation and creating a parental minefield. **The wall street journal**. June 18, 2019. Available at: <https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201> Accessed 10 Ago., 2021.

JEEVANJEE, Kiran K., Nice Thought, Poor Execution: why the dormant commerce clause precludes California's CCPA from setting national privacy law, 70 **AM. U. L. REV**. F. 75, 2020.

KATZ, Jonathan; FENER. Is a YouTube COPPAcalypse Coming? FTC Rules Could

Start Demonetizing Creators in 2020, **TUBEFILTER**. Nov. 5, 2019. Available at: <https://perma.cc/D6CL-WGQR> Accessed 09 Jul., 2021.

KEARNS, Michael; ROTH, Aaron. **The ethical algorithm**: the science of socially aware algorithm design. NEW YORK: Oxford University Press, 2019.

KOOPS, Bert-Jaap; NEWEKKI, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tom; GALIČ, Maša, A typology of privacy (March 24, 2016). **University of Pennsylvania Journal of International Law 38(2)**, p. 483-575 (2017); Tilburg Law School Research Paper No. 09/2016, p. 2. Available at <https://ssrn.com/abstract=2754043> Accessed 25 Mar., 2018.

KRISTOL, David. M. HTTP Cookies: standards, privacy, and politics. **ACM Transactions on Internet Technology**, Vol. 1, #2, November 2001 Available at: <https://doi.org/10.48550/arXiv.cs/0105018> Accessed 29 Aug., 2022.

LANDESBERG, Martha K., LEVIN, Toby Milgrom; CURTIN, Caroline G.; LEV, Ori., **Federal Trade Commission, Privacy Online**: a report to congress (1998), p. 42. Available at <https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf> Accessed 10 Ago., 2021.

LESSIG, Lawrence. **Code and Other laws of cyberspace**. Basic Books: New York, 1999.

LI, Yunge. The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth, 32 **LOY. Consumer Rev.** 177, 2019.

LIMA MARQUES, Claudia. **Comentários ao Código de Defesa do Consumidor**, 2ª edição, Editora Revista dos Tribunais, 2006.

LLOYD, Ian J. **Information Technology law**. 7 ed. OXFORD: Oxford University Press: 2014.

LOCKE, John. **Second Treatise of Government** §27, at 19 (1980) (1690).

LOCKE, John. **According to the civil government treaty.** Translation: Magda Lopes and Marisa Lobo da Costa. Voices Publishing House. Available at: <http://www.xr.pro.br/if/locke-segundo_tratado_sobre_o_governo.pdf> Accessed 11 Ago., 2018.

MARMOR, Rachel R. et al., Copycat CCPA: bills introduced in states across country, **DAVIS WRIGHT TREMAINE LLP** (Feb. 8, 2019). Available at: <https://www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou> Accessed 12 Jul., 2021.

MARQUES, Claudia Lima. Diálogo das Fontes in BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual do Direito do Consumidor.** 5 ed. Ver., atual. E ampl. São Paulo: Editora Revista dos Tribunais: 2013.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2014.

MASON, Alpheus Thomas. **Brandeis**: A free man's life. William s Hein & Co: Reprint edition (June 30, 2007).

MATECKI, Lauren A., Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era, 5 **Nw. J.L. & SOC. POL'Y** 369, 370 (2010).

MATLICK, Justin. The Future of the Net: Don't Restrain Trade in Information, **WALL ST. J.,** Dec. 2, 1998.

MCCARTHY, J. Thomas. **The Rights of Publicity and Privacy.** §5.59 (2d ed. 2005).

MELLO Jr., John P. Data breaches affected nearly 6 billion accounts in 2021. **TechNewsWorld**. Jan 18, 2022. Available at <https://www.technewsworld.com/story/data-breaches-affected-nearly-6-billion-accounts-in-2021-87392.html> Accessed 18 May, 2022.

MILL. John Stuard. **On Liberty**, 1859. Chapter I. Available at <https://www.utilitarianism.com/ol/one.html> Accessed 11 Ago., 2018.

MILLER, Arthur. **The assault on privacy**. Ann Arbor: University of Michigan, 1971, p. 63

MILLER, Richard E. **On the End of Privacy**: Dissolving Boundaries in a Screen-Centric World (Composition, Literacy, and Culture). University of Pittsburgh Press, 2019, p. 233

MILLER, Richard E. **On the End of Privacy**: Dissolving Boundaries in a Screen-Centric World (Composition, Literacy, and Culture). University of Pittsburgh Press, 2019.

MOORE, Adam D. **Privacy rights**: moral and legal foundations. Pennsylvania: The Pennsylvania State University Press, 2010.

MULLIGAN, Stephen. **Data Protection and Privacy Law**: An Introduction. Congressional Research Service (CRS), 2019. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11207> Accessed 01 Mar., 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines for Media Sanitization**. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf> Acessed 02 May, 2022.

NEWMAN, Lily Hay. If You Want to Stop Big Data Breaches, Start with Databases. **WIRED** (Mar. 29, 2017), https://www.wired.com/2017/03/want-stop-big-data-breaches-startdatabases/

NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. New York: New York University Press, 2018.

O'BRIEN, David. **Privacy, Law, and Public Policy**, 15, 16 in SOLOVE, Daniel J. Understanding privacy. Cambridge, Massachusetts: Harvard University Press. 2008.

O'NEIL, Cathy. **Weapons of Math Destruction**: how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

O'DONNELL, Anna. Why the VPPA and COPPA Are Outdated: how Netflix, YouTube, and Disney+ can monitor your family at no real cost. **Georgia Law Review**, vol. 55, no. 1, Fall 2020, p. 490.

OHM, Paul. Broken Promises of Privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Vol. 57, p. 1701, 2010

OLINDER, Nina; TSVETKOV, Alexey; FEDYAKIN, Konstantin; ZABURDAEVA, Kristina. Using digital foorprints in social research: an interdisciplinary approach. **Wisdom** 3(16), 2020, p. 127. Available at <https://cyberleninka.ru/article/n/using-digital-footprints-in-social-research-an-interdisciplinary-approach/viewer> Accessed in 31 Aug., 2022.

OLIVIERO, Maurizio; CRUZ, Paulo Márcio. Reflexões sobre o direito transnacional. **Revista Novos Estudos Jurídicos.** Itajaí, v. 17, n. 1, p. 18-28, 2012. Ver também CRUZ, Paulo Márcio & BODNAR, Zenildo. O novo paradigma de Direito na pós-modernidade. Porto Alegre - RECHTD/UNISINOS. **Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito**, v. 3, p. 75-83, 2011 e CRUZ, Paulo Márcio;

O'REILLY, James. **FEDERAL PREEMPTION OF STATE AND LOCAL LAW**: legislation, regulation, and litigation 8 (2006), Available at: <http://apps.americanbar.org/abastore/products/books/abstracts/5010047samplechpabs.pdf> Accessed 09 Jul., 2021.

Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos**, em 10/12/1948. Available at <http://www.ohchr.org/EN/UDHR/Pages/UDHRIndex.aspx>. Accessed 25 Mar., 2018.

PANORAMA MOBILE TIME/OPINION BOX - **Crianças e smartphones no Brasil.** Outubro de 2019. Available at: <https://www.mobiletime.com.br/ pesquisas/criancas-e-smartphones-no-brasil-outubro-de-2019/> Accessed 29 Jun., 2021.

PARENTALRIGHTS. **The Convention on the Rights of the Child Is Back in Congress**. March 3, 2020. Available at: <https://parentalrights.org/convention-on-the-rights-back/> Accessed 06 Aug., 2022.

PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica:** Teoria e Prática. 14.ed.rev.atual. e amp. Florianópolis: EMais, 2018.

PCOMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br. Pesquisa sobre o uso da

internet por crianças e adolescentes no Brasil: TIC kids online Brasil 2017. Survey on internet use by children in Brazil: ICT kids online Brazil 2017 [livro eletrônico] / Núcleo de Informação e Coordenação do Ponto BR, [editor]. -- São Paulo: **Comitê Gestor da Internet no Brasil,** 2018. Available at: <https://cetic.br/media/docs/publicacoes/2/tic_kids_online_2017_livro_eletronico.pdf> Accessed 05 Apr., 2019.

PEASLEY, Mark. It's Time for an American (Data Protection) Revolution, 52 **AKRON L. REV**. 911, 943 (2018).

Piaget, Jean. **O juízo moral na criança** (E. Lenardon, Trad.). São Paulo, SP: Summus. 1994. (Original published in 1932)

PICARD, Rosalind Wright. **Affective computing**. Cambridge, MA: MIT Press, 1997.

POSNER, Richard. An economic theory of privacy. **Georgia Law Review**, 3/1978, 9. 393-422, p. 394. Same meaning in POSNER, Richard. Privacy, secrecy and reputation. In: **Buffalo Law Review**, 28 (winter) 1979.

POSNER, Richard. The Economics of Justice. **Harvard University Press**. January 1, 1981.

PRIORIDADE ABSOLUTA. **Panorama**: dados sobre a infância e adolescência brasileiras. Available at <https://prioridadeabsoluta.org.br/estatuto-crianca-adolescente/panorama-infancia-adolescencia/> Accessed 09 May, 2022.

PROSSER, William L. Privacy. **California Law Review**, vol. 48. August 1960, n. 3, p. 383. Available at <https://doi.org/10.15779/Z383J3C> Acessed 15 Ago., 2019.

QUEIROZ, Sávio Silveira, RONCHI, Juliana Peterle e TOKUMARU, Rosana Suemi. Constituição das Regras e o Desenvolvimento Moral na Teoria de Piaget: Uma reflexão Kantiana. **Psicologia**: Reflexão e Crítica, 22(1), 69-75, 2009.

REIMAN, Jeffrey H.. Privacy, Intimacy, and Personhood in SCHOEMAN, Ferdinand D. **Philosophical Dimensions of Privacy:** an anthology, CAMBRIDGE*:* Cambridge University Press, 1984.

RICHARDSON, Megan. **The right to privacy**. Origins an influence of a nineteenth-century idea. Cambridge University Press: 2017.

ROMANI, Bruno. **Vazamento de dados**: Informações de Bolsonaro e ministros do STF estão à venda na internet. Estadão. Available at <https://link.estadao.com.br/noticias/cultura-digital,dados-de-bolsonaro-e-ministros-do-stf-estao-a-venda-na-internet-apos-megavazamento,70003600653> Accessed 18 May, 2022.

ROSENBERG, Jerry M. **The Death of Privacy**. Random House, 1969.

RUIZ MIGUEL, Carlos, **La configuracion constitucional del derecho a la Intimidad**. Doctoral thesis. Universidad Complutense de Madrid, June 15, 1992.

Available at <https://perma.cc/5YR4-2679> Accessed 11 Ago., 2018.

SAFIER, Seth, Between Big Brother and the Bottom Line: Privacy in Cyberspace, 5 **VA. J.L. & TECH.** 6, 29 (2000).

SARTRE, J.-P. L'etre et le neant (Paris, 1953), Part 3, Le pour-autrui. In BENN, Stanley I. **A theory of freedom**. CAMBRIDGE: Cambridge University Press, 1988.

SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone. The Crisis of Consent: fow stronger legal protection may lead to weaker consent in data protection. **16 Ethics & Info**. Tech. 171, 2014

SCHEUERMAN, William E. Whistleblowing as civil disobedience: the case of Edward Snowden. **Philosophy & Social Criticism**, v. 40, n. 7, 2014.

SCHNEIDER, Harvey A. Katz v. United States: **The Untold Story**. 2009. Available at <http://www.mcgeorge.edu/Documents/Publications/06_Schneider_Master1MLR40.pdf> Accessed 12 Ago. 2018.

SCHNEIDER, Harvey A... **Official transcript of the trial section**, 00:13:32, Available at <https://apps.oyez.org/player/#/warren15/oral_argument_audio/15388> Accessed 11 Ago., 2018.

SCHWARTZ, Paul. Privacy and Democracy in Cyberspace, 52 **VAND. L. REV**. 1609-1663, 2001

SCHWARTZ, Paul. SOLOVE, Daniel. Overview of Fair Information Practice Principles (FIPPs) in THE AMERICAN LAW INSTITUTE. **Principles of the Law Data Privacy**: tentative draft. April 15, 2019. Submitted by the Council to the Members of The American Law Institute for Consideration at the Ninety-Sixth Annual Meeting on May 20, 21, and 22, 2019. Content Downloaded from HeinOnline.

SEGARRA, Lisa Marie. **Mark Zuckerberg Just Revealed 3 Steps Facebook Is Taking to Address the Cambridge Analytica Crisis Time**. March 21, 2018. Available at <https://time.com/5209729/mark-zuckerberg-facebook-cambridge-analytica/#:~:text=The%20good%20news%20is%20that,step%20up%20and%20do%20it.%E2%80%9D> Accessed 18 May, 2022.

SIMILARWEB. **Top Websites Ranking.** Available at: <https://www.similarweb.com/top-websites/> Accessed 09 Jul., 2021. Ranking method can be found at: <https://www.similarweb.com/corp/ourdata/> Accessed 09 Jul., 2021.

SMITH, Nicole. Protecting Consumers in the Age of the Internet of Things, 93 ST. **JOHN'S L. REV**. 851, 866 (2019).

SNOWDEN, Edward. Edward Snowden: a right to privacy is the same as freedom of speech – video interview. **The Guardian.** Available at: <https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video> Accessed 01 Mar., 2018.

SOLOVE, Daniel J.; ROTENBERG, Marc. SCHWARTZ, Paul M. **Information Privacy** Law 31 (2d ed. 2006).

SOLOVE, Daniel. **Nothing to hide**: the false tradeoff between privacy and security. New Haven & London: Yale University Press, 2011.

SOLOVE, Daniel. Privacy Self-management and the Consent Dilemma, in: **Harvard Law Review**, vol. 126, 2013, 1880-1903. p. 1880.

SOLOVE, Daniel. The Legacy of Privacy and Freedom, vii, in PROSSER, William L. Privacy. **California Law Review**, vol. 48. August 1960, n. 3, p. 383. Available at <https://doi.org/10.15779/Z383J3C>. Accessed 15 Aug., 2019. Also in Katz v. United States, 389 U.S. 347 (1967) Harlan, J., concurring.

SOLOVE, Daniel. **Understanding privacy**. Cambridge, Massachusetts: Harvard University Press. 2008.

SOLOVE, Daniel., **Nothing to hide**: the false tradeoff between privacy and security. United States: Yale University Press, 2011.

SOLOVE, Daniel; KEATS CITRON, Danielle. Risk and Anxiety: a theory of data-breach harms. **Texas Law Review**, vol. 96, no. 4, March 2018, p. 737-786, p. 785.

SOLOVE, Daniel; KEATS CITRON, Danielle. Risk and Anxiety: a theory of data-breach harms. **Texas Law Review**, vol. 96, no. 4, March 2018, p. 745.

STAFFEN, Márcio Ricardo. **Interfaces do Direito Global.** 2. ed. ampl. atual. Rio de Janeiro: Lumen Juris, 2018.

STALLA-BOURDILLON, Sophie; KNIGHT, Alison Knight. Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. **Wisconsin International Law Journal**, vol. 34, no. 2, Winter 2016, p. 284-322. HeinOnline.

STATE LEGAL AGES LAWS. Available at: <https://statelaws.findlaw.com/family-laws/legal-ages.html> Accessed 09 Jul., 2021.

SYKES, Charles J. **The End of Privacy**: The Attack on Personal Rights at Home, at Work, On-Line, and in Court. St. Martin's Press, 1999.

TGARFINKEL, Simson. **The Death of Privacy in the 21st Century**. O'Reilly Media, 2008.

The OECD Privacy Framework 2013. **The evolving privacy landscape**: years after the OECD Privacy Guidelines (2011), p. 67-68. Available at: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Accessed 15 Mar., 2021.

THE WHITE HOUSE. **A Framework for Global Electronic Commerce**. 1 July 1997. Available at

<https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>. Accessed 11 May, 2022.

THOMSON, Judith Jarvi. **The Right to Privacy**, in Philosophical Dimensions of Privacy: An Anthology 272, 272 (Ferdinand David Schoeman ed., 1984).

U.S. DEP'T COM. **Welcome to the U.S.-EU Safe Harbor**. (Jan. 26, 2017, 12:38 PM), Available at <http://2016.export.gov/safeharbor/eu/eg_main_018475.asp> [hereinafter Safe Harbor Overview] Accessed 04 Sep., 2021.

U.S. DEPARTMENT OF HOMELAND SECURITY. **PRIVACY POLICY GUIDANCE MEMORANDUM**. Washington, DC. Memorandum Number: 2008-01. Available at <https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf> Accessed 13 Jan., 2022.

U.S. GOVERNMENT PRINTING OFFICE. **Children's Online Privacy Protection Act of 1998**, S. 2326, 105th Cong. §3(a) (1998). Available at: <https://www.congress.gov/bill/105th-congress/senate-bill/2326/text> Accessed 10 Ago., 2021.

UCLA Fielding School of Public Health. **A global report card**: Are children better off than they were 25 years ago? Available at: <https://ph.ucla.edu/news/press-release/2014/nov/global-report-card-are-children-better-they-were-25-years-ago> Accessed 25 Jul., 2022.

UNICEF. **Convenção sobre os Direitos da Criança**. Brasília: UNICEF, 1989. Available at: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca> Accessed 09 May, 2022.

UNITED NATIONS CHILDREN'S FUND (UNICEF). **The Case for Better Governance of Children's Data**: a Manifesto. May 2021, p. 52 Available at: <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto> Accessed 05 Jul., 2022.

UNITED NATIONS CHILDREN'S FUND (UNICEF). **The Case for Better Governance of Children's Data**: a Manifesto. May 2021, p. 52 Available at: <https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto> Accessed 05 Jul., 2021.

UNITED NATIONS. **Committee on the Rights of the Child**. Available at: https://www.ohchr.org/en/treaty-bodies/crc Acess in: 24 jul. 2022.

UNITED NATIONS. **Convention for the Protection of Human Rights and Fundamental Freedoms** on 04/11/1950. Available at: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Accessed 25, Mar., 2018.

UNITED NATIONS. **Convention on the Rights of the Child**. New York, 20 November 1989 STATUS AS AT: 24-07-2022 09:16:08 EDT. Available at: <https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2

&mtdsg_no=IV-11&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.

UNITED NATIONS. **Convention on the Rights of the Child**. New York, 20 November 1989 STATUS AS AT: 24-07-2022 09:16:08 EDT. Available at: <https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2&mtdsg_no=IV-11&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.;

UNITED NATIONS. **Convention on the Rights of the Child**. New York, 25 May 2000, 11.c Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Available at: <https://treaties.un.org/pages/ShowMTDSGDetails.aspx?src=UNTSONLINE&tabid=2&mtdsg_no=IV-11-c&chapter=4&lang=en#Participants> Accessed 24 Jul., 2022.

UNITED STATES. **Child Status Protection Act.** PUBLIC LAW 107–208—AUG. 6, 2002 116 STAT. 927. Available at: <https://www.congress.gov/107/plaws/publ208/PLAW-107publ208.pdf> Accessed 07 Jul., 2021.

VAN DER HOF, Simone. Agree... Or do I?: a rights-based analysis of the law on children's consent in the digital world. **Wisconsin International Law Journal**, vol. 34, p. 101-136, 2016.

VERBLE, Joseph. The NSA and Edward Snowden: surveillance in the 21st century. **ACM SIGCAS Computers and Society**, v. 44, n. 3, 2014.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review** 4, no. 5: 1890.

WESTIN, Alan. **Privacy and freedom**. New York: Atrtheneum Publishers, 1967.

WHITAKER, Reg. **The End of Privacy**: How Total Surveillance Is Becoming a Reality. New Press, 2000.

WHITMAN, James. The Two Western Cultures of Privacy: Dignity versus Liberty. **Yale Law Journal**, vol. 113, no. 6, April 2004, p. 1151-1222. HeinOnline., p. 2004.

WICKER, Stephen B. **Cellular Convergence and the Death of Privacy**. Oxford University Press, 2013.

YOUTUBE. **Central de ajuda**. Available at: <https://support.google.com/YouTube/answer/1646861?hl=pt-BR#:~:text=Mesmo%20que%20voc%C3%AA%20j%C3%A1%20tenha,um%20computador%20ou%20dispositivo%20m%C3%B3vel> Accessed 09 Jul., 2021.

YOUTUBE. **Our comment on COPPA**. Dec.09.2019. Available at: <https://blog.YouTube/news-and-events/our-comment-on-coppa/> Accessed 06 Ago., 2021.

YOUTUBE. **Perguntas frequentes sobre conteúdo para crianças**. Available at: <https://support.google.com/YouTube/answer/9684541?hl=pt-

BR&ref_topic=9689353#zippy=%2Cquais-recursos-n%C3%A3o-est%C3%A3o-dispon%C3%ADveis-em-conte%C3%BAdo-para-crian%C3%A7as-por-que-essas-funcionalidades-foram-removidas> Accessed 09 Jul., 2021.

YOUTUBE. **YouTube Help**: Set Your Channel or Video's Audience, GOOGLE. Available at: <https://support.google.com/YouTube/answer/9527654> Accessed 09 Jul., 2021.

ZELLER, Tom. AOL Executive Quits After Posting of Search Data, **N.Y. TIMES**, Aug. 22, 2006. Available at <http://www.nytimes.com/2006/08/22/technology/22iht-aol.2558731.html> Accessed 13 Apr., 2020.

ZUBIZARRETA, Juan Hernández. **Las empresas transnacionales frente a los derechos humanos**: história de una asimetría normativa. Bilbao: Hegoa, 2009.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. PUBLICAFFAIRS: New York, 2019.

LIST OF LAWS

U.S

104 Stat. 996 (Children's Television Act of 1989)

15 U.S.C. § 1681 (Fair Credit Reporting Act)

15 U.S.C. §§ 6501-6506 (Children's Online Privacy Protection Act)

15 USC § 6801 et seq., (Gramm-Leach-Bliley Act of 1999)

16 CFR §§ 313, 314 (Privacy of Consumer Financial Information)

16 CFR Part 312 (Children's Online Privacy Protection Rule)

18 U.S.C. § 1030 (Fraud and related activity in connection with computers)

18 U.S.C. § 2518 (Electronic Communications Privacy Act of 1986).

45 C.F.R. § 164 (Security and privacy)

47 U.S.C. § 151 et seq. (The Communications Act of 1934)

5 U.S.C § 552a (Privacy Act of 1974)

Cal. Civ. Code §§ 1798.100-199 (California Consumer Privacy Act of 2018)

45 CFR §§ 160, 162, 164) (HIPAA Privacy Rule of 1996)

BRAZIL

BRASIL. CONSELHO NACIONAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE – CONANDA. **Resolução 163/2014**. Dispõe sobre a abusividade do direcionamento de publicidade e de comunicação mercadológica à criança e ao adolescente.

BRASIL. Lei complementar nº 105, de 10 de janeiro de 2001. **Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências**.

BRASIL. Lei nº 9.296/1996 de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.**

BRASIL. Lei nº 10.406 de 10 de janeiro de 2002. **Código Civil.**

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet** (MCI).

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais** (LGPD).

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de defesa do consumidor** (CDC).

BRASIL. Lei. n. 5.172, de 25 de outubro de 1966. **Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios.**

BRASIL. **Constituição política do Império do Brasil**, de 25 de março de 1824.

OTHER REGULATIONS

DHS – Fair Information Practice Principles (2008)

U.S. DEPARTMENT OF HOMELAND SECURITY. **PRIVACY POLICY GUIDANCE MEMORANDUM**. Washington, DC. Memorandum Number: 2008-01. Available at <https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf> Accessed 13 Jan., 2022.

EU Data Protection Directive (1995)

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). **EU Data Protection Directive.** Jornal Oficial da União Europeia, Estrasburgo, 24/10/1995. Available at: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046> Accessed 15 May, 2019.

EU General Data Protection Regulation (2016)

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 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). **GDPR.** Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Available at: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Accessed 16 Apr., 2019.

FTC – Privacy Framework and Implementation Recommendation (2012).

FEDERAL TRADE COMMISSION. **Protecting Consumer Privacy in an Era of Rapid Change**: Recommendations For Businesses and Policymakers, march 2012. Available at: <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> Accessed 01 Jun., 2022.

HEW – The Code of Fair Information practices (1973)

U.S. DEP'T. OF HEALTH, EDUCATION AND WELFARE. Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the

Rights of Citizens. **The Code of Fair Information practices** (1973).

OECD – Privacy Principles (1980)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The OECD privacy framework**. Available at: <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> Accessed 15 Feb., 2019.

PIPEDA (Schedule 1) (2000)

CANADA. Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). **PIPEDA**. Available at: <https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html> Accessed 21 Mar., 2019.

THE WHITE HOUSE – Consumer Privacy Bill of Rights (2012)

THE WHITE HOUSE. Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy. **Consumer Privacy Bill of Rights.** February, 2012. Available at: <https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf> Accessed 05 Mar., 2019.

LIST OF CASES

U.S

Pope v. Curl, 26 eng. rep. 608 (1741)

Prince Albert v Stange 64 ER 293 (1848)

DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881)

Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)

Olmstead v. United States, 277 U.S. 438 (1928)

Griswold v. Connecticut, 381 US 479 (1965)

Katz v. United States, 389 U.S. 347 (1967)

Eisenstadt v. Baird, 405 US 438 (1972)

Roe v. Wade, 410 US 113 (1973)

United States v. Miller, 425 U. S. 435 (1976)

See Smith v. Maryland, 442 U. S. 735 (1979)

Planned Parenthood v. Casey, 505 US 833 (1992)

Roper v. Simmons, 543 U.S. 551 (2005)

Graham v. Florida, 560 U.S. 48 (2010)

Miller v. Alabama, 567 U.S. 460 (2012)

Carpenter v. United States, 585 U.S. (2018)

BRAZIL

Ação Civil Pública n. 1054077-72.2019.8.26.0002 (MP-SP x Mattel do Brasil Ltda)

Ação Civil Pública n. 1132354-36.2018.8.26.0100 (MP-SP x Google Brasil Internet Ltda)

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1348532.** Relator: Ministro Luis Felipe Salomão, j. 10.10.2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1558086**. Relator: Ministro Humberto Martins, j. 10.03.2016

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416**. Tribunal Pleno, j. 10.05.2006.