Journal of Intellectual Property Studies
Vol. 5 (01), January 2022, pp. 109-130

CIVIL LIABILITY IN THE PROCESSING AND PROTECTION OF PERSONAL DATA BY AI APPLICATIONS IN EUROPE AND BRAZIL

BRUNA WERLANG PAIM* AND LUKAS RUTHES GONÇALVES**

Abstract

Data processing operations can already be performed by AI (Artificial Intelligence) applications. Currently, the phenomenon of "robotic bosses" is already considered i.e., AI applications that are effectively responsible for managing customer data and deciding the best course of action for a given company or association. With the addition of data protection laws such as the Brazilian General Law on Personal Data Protection (LGPD) and the European General Data Protection Regulation (GDPR) this type of operation already fits into the functions of controllers and operators, who can be held legally responsible for their acts. In this sense, this article aims to verify, first of all, what these AI applications would be and, what are the attributions of data controllers and operators according to LGPD and GDPR. Soon afterwards, it will be verified the Civil Liability regime in Europe and Brazil regarding the topic in order to finally address what would be the civil liability of a non-human data processing agent. As a conclusion, it is clear that an AI application is just a tool and that the liability would fall on the natural person operator or controller, especially on the second.

* Lawyer, Specialist in Law, Logistics and International Business, and graduated from Pontifícia Universidade Católica do Paraná (PUCPR). Researcher at the Advanced Study Group on International Law and Sustainable Development (NEADI), registered at CNPQ.
** Lawyer, Doctorate candidate and Master in Intellectual Property Law from Universidade Federal do Paraná (UFPR). Researcher at the Group for the Study of Copyright and Industrial Law (GEDAI), registered at CNPQ.

I. INTRODUCTION

By providing for significant administrative sanctions, such as fines of up to fifty million reais per violation in the case of the LGPD, the civil liability of data processing agents becomes the subject of relevant debate.

Regardless of the field, the use of artificial intelligence applications is growing considerably. However, when used for processing personal data, the application of AI brings with it not only the facilities of innovation but also the legal uncertainties of what is still considered a novelty.

Thus, since the law requires dialogue with other areas of science, it is imperative to understand what artificial intelligence is and how it works, and the first chapter will be dedicated to this subject. Next, we will address the data processing agents according to the Brazilian LGPD (Lei Geral de Proteção de Dados) and the GDPR (General Data Protection Regulation) of the European Union, thus exploring the roles and responsibilities of the controller and operator of personal data. In the third chapter, in a comparative analysis, we will seek to verify how civil liability occurs in Brazil and in European legislation, taking German law as a reference, considering the lack of a European civil law. Then, considering the previously exposed topics, we will present reflections about civil liability in cases which artificial intelligence appears as an agent of personal data treatment.

II. THE THREE ESSENTIAL ELEMENTS THAT MAKE UP AN AI APPLICATION: SOFTWARE, HARDWARE, AND DATA

In order to explore how an AI application could be used in personal data processing operations, it is necessary to first understand how such a program operates and what elements make its operation possible. A precise understanding of what Artificial Intelligence technology is all about is of fundamental importance to understanding some of the challenges its regulation presents.

Russell and Norvig, authors of one of the most cited books on AI,[1] define Artificial Intelligence as being "the study and design of intelligent agents, where an intelligent agent is a system that perceives its environment and performs actions that maximize its chances of success."[2] Following this same line of thought, Kurzweil, a renowned American inventor and futurist,

[1] STUART RUSSEL & PETER NORWIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH, 4 PEARSON (2021).
[2] STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH, 3 PRENTICE HALL (2010).

approaches this technology as being "the art of creating machines that perform functions that require intelligence when performed by people."[3]

These are just two of several definitions that this concept has and that has been gaining even more fame in recent times. However, the concept of Artificial Intelligence to be adopted for the purposes of the present paper is as follows:

> It is an area of study focused on solving problems (or creating machines that perform this function) that previously only the human mind could answer. Thus, it is not possible to say that there is "one" or "the" Artificial Intelligence. What does exist is a number of different applications that make use of advanced technology in order to supplement the human reasoning capacity in one use or another.[4]

In other words, an Artificial Intelligence application is a program that runs on some kind of computer and emulates human reasoning based on the information it receives. We will see more about the elements that compose this type of application in the items below.

Within this area of study, there is also an important discussion about the distinction between the existing modalities of AI applications. In the existing literature on the subject, four types are popularly found: *narrow* as opposed to *general AI* and *weak* as opposed to *strong AI* (also called AGI: *Artificial General Intelligence*).

Teemu Roos says that *Narrow* refers to an AI application capable of performing a single task. *General, on the* other hand, would be a machine capable of handling any activity of the intellect. All Artificial Intelligence methods used today are characterized as *Narrow*.[5] That is, they are applications that are programmed for a single purpose and can only execute that single purpose. *General AI*, which can perform any task regardless of whether it has been programmed or not, is in the realm of science fiction.

The dichotomy between *weak* and *strong*, on the other hand, can be narrowed down to the philosophical distinction between appearing intelligent through your actions and actually being intelligent, as problematized by the Turing Test.[6] According to Teemu Roos, *strong AI* would amount to a genuinely intelligent and self-aware mind. *Weak AI*, on the other hand, would be

---

[3] RAYMOND KURZWEIL, THE AGE OF INTELLIGENT MACHINES (MIT Press 1990).
[4] Lukas Ruthes Gonçalves, *A Tutela Jurídica de Trabalhos Criativos Feitos por Aplicações de Inteligência Artificial no Brasil*, (MAR. 27, 2019) (unpublished M. Sc. dissertation, Universidade Federal do Paraná 2019), https://bit.ly/2YLBgnN.
[5] ELEMENTS OF AI, https://www.elementsofai.com (last visited Aug. 18, 2018).
[6] A.M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950) (According to the Turing test, an interviewer would interrogate two players, a person and a computer, without knowing their identity, in order to determine if the computer could successfully make the interviewer think that it is human. If successful, this would be proof that a machine could indeed be endowed with intelligence).

what effectively exists, namely systems that exhibit intelligent behaviour despite being just computer applications.[7]

It is important to notice that "even if humanity is not close to developing an AGI that has its own consciousness, its application in a narrow way is already quite widespread in society, even if in a not so evident way".[8] Thus, this type of *narrow* application does not prevent existing programs from already having the ability to make decisions based on the information they receive, as will be discussed throughout this paper.

Examples of current uses of AI applications that are already having an effect on society and the contemporary business environment include selection and recruitment of candidates by analysing resumes of current employees, training employees from the use of AI applications in conjunction with augmented reality devices, managing repetitive activities to increase worker productivity, and monitoring the quantity and quality of work performed by employees through AI applications and IoT (Internet of Things) devices.[9]

Thus, the definition of AI was approached as being the area of study dedicated to creating devices that successfully emulate human reasoning, such as those that influence the process of hiring employees or helping a company to make decisions. Now we will talk about the main elements that enable the proper functioning of an application of this type, which are three: software, hardware, and data.

A. Software

To talk about software, let's first glance at another definition of AI. According to McCarthy, AI is the "theory and development of computer systems capable of performing tasks which would normally require human intelligence, such as visual perception, speech recognition, decision making, and translation between languages".[10] The key term in this definition is "computer systems", which are nothing more than programs, or software composed of algorithms.

---

[7] ELEMENTS OF AI, *supra* note 5.
[8] Gonçalves, *supra* note 4, at 35.
[9] Bernard Marr, *Artificial Intelligence in the Workplace: How AI is Transforming your Employee Experience*, FORBES (MAY 29, 2019), https://www.forbes.com/sites/bernardmarr/2019/05/29/artificial-intelligence-in-the-workplace-how-ai-is-transforming-your-employee-experience/#6f75fcb153ce.
[10] JOHN MCCARTHY ET. AL., PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE (1955).

The algorithm "is a set of mathematical instructions, a sequence of tasks to achieve an expected result in a limited amount of time".[11] In other words:

> Its existence is not necessarily linked to a computer or other electronic device, so that a cake recipe, for example, can be considered an algorithm for the physical world, because it is a series of instructions to achieve a certain end.[12]

According to Solomon Gandz, the term is also the Latinization of the name of a Persian mathematician from the 9th century named Al-Khwãrizmi, who taught in his works mathematical techniques to be solved manually, and was responsible for presenting the first solution of linear and quadratic equations.[13]

Turning to the field of computing, according to Cormen et al., an algorithm would be defined as "any well-defined computational procedure that takes some value or set of values as input and produces some value or set of values as output".[14]

On this topic, it was previously stated:

> Such a set of instructions that transforms a given input value into an output result can be realized through lines of code that when applied to a given machine perform specific actions. Such lines of code constitute, fundamentally, a computer program.[15]

When used in AI applications that draw on Machine Learning, one is looking for "algorithms that can learn and make predictions about data – these algorithms follow strictly static instructions when making predictions or decisions based on data by building a model from sample inputs".[16]

In other words, AI applications that make use of the Machine Learning techniques are computer programs that produce a certain output value that emulates human reasoning based on the information provided to it as input value. This means that the way in which such an application receives and manages this data that serves as *input* is extremely important, as will be seen below.

From the application of the Machine Learning technique has developed a new, more complex programming modality called *Deep Learning*. It uses artificial neural networks (simplified

---

[11] Dora Kaufman, *Os meandros da Inteligência Artificial: conceitos-chave para leigos*, ASSOCIAÇÃO BRASILEIRA DE LAWTECHS & LEGALTECHS (FEB. 22, 2018), https://ab2l.org.br/os-meandros-da-inteligencia-artificial-conceitos-chave-para-leigos/.
[12] Gonçalves, *supra* note 4, at 44.
[13] Solomon Gandz, *The Origin of the Term "Algebra"*, 33 AM. MATHEMATICAL MONTHLY 437 (1926).
[14] THOMAS H. CORMEN ET. AL, ALGORITMOS TEORIA E PRÁTICA 3 (Vandenberg D. de Souza trans., Campus 2nd ed. 2002).
[15] Gonçalves, *supra* note 4, at 45.
[16] Kaufman, *supra* note 11.

simulations of how biological neurons behave) to extract rules and patterns from given data sets.[17]

This technology consists of a series of neuron-like units that combine a series of input values to produce an output value. This output, in turn, is also passed to other neural units, following a chain.[18] Thus, "an application using *Deep Learning* will, in the first step, analyse a sequence of data to arrive at a certain pattern; it will then pass that pattern through a second layer of analysis to arrive at a more refined pattern, and so on".[19]

Temu Roos states that it is precisely this depth of layers that allows the network to learn more complex structures without requiring unreasonably excessive amounts of data. Furthermore, the author points out that another big reason for building artificial neural networks would be to use the biological systems present in humans as inspiration to program better AI programs. According to him:

> The case of neural networks in general, as an AI approach, is based on an argument similar to that of logic-based approaches. In the latter case, it was thought that in order to achieve human-level intelligence, we need to simulate higher-level thought processes and, in particular, the manipulation of symbols representing certain concrete or abstract concepts using logical rules.[20]

In summary, we showed that an Artificial Intelligence application consists of software, whose algorithm is made by means of techniques that best emulate human thinking (*Machine Learning* and *Deep Learning*). It is now necessary to verify where this type of program is executed to have an effect in the physical world.

B. Hardware

Hans Moravec makes an analogy that an AI application would need computing power in the same way that airplanes need horsepower. Below a certain threshold the technology would not

[17] *How Machine Learning Works*, THE ECONOMIST (MAY 14, 2015), https://www.economist.com/the-economist-explains/2015/05/13/how-machine-learning-works?fsrc=scn/fb/te/bl/ed/.
[18] NAT'L SCI. AND TECH. COUNCIL, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE, at 9 (2016). National Science and Technology Council. Washington, D.C. 20502, p. 9.
[19] Gonçalves, *supra* note 4, at 46.
[20] ELEMENTS OF AI, *supra* note 5.

work, but as the power increases the task becomes easier. In this sense the area of hardware is one that is, fortunately, constantly improving.[21]

Companies like Microsoft have been developing so-called Quantum Computers, which promise to considerably improve the analysis capacity that current machines allow.[22] For comparison "in 1997, IBM's Deep Blue analysed 200 million moves per second to outperform chess champion Garry Kasparov. A quantum machine, on the other hand, would be able to analyse 1 trillion moves every second."[23]

This is because the difference would be in the way a quantum computer works.[24] An analysis made by the quantum computing team at Microsoft states that the processing in a traditional computer occurs in a binary way, with information being transmitted from *bits* that can only have a binary value of 0 or 1, which limits the processing capacity. In quantum computing, a *quantum bit* can hold both values at the same time, which is called a superposition state, and this allows the processing speed to be vastly superior compared to traditional computers.[25]

Faster Hardware would also make it possible to solve another technological barrier explained by what is called the Moravec Paradox. This is the observation "that complex mental problems require low computational capacity to be replicated and that motor activities of low degree of complexity (such as holding a glass) would, conversely, require enormous resources."[26] According to Moravec:

> It is comparatively easy to make computers exhibit adult-level performance in intelligence tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old child when it comes to perception and mobility.[27]

This difficulty is justified "by the fact that these apparently simpler activities require a large amount of data to be performed, but that are not perceived by the human consciousness".[28] However, for activities that are considered complex, such as information analysis and

---

[21] Hans Moravec, The Role of Raw Power in Intelligence (May 12, 1976) (unpublished manuscript), https://frc.ri.cmu.edu/~hpm/project.archive/general.articles/1975/Raw.Power.html.
[22] Gonçalves, *supra* note 5, at 49.
[23] Filipe Garrett, *Computador e processador quântico: sete coisas que você precisa saber*, TECHTUDO (MAR. 26, 2018), https://www.techtudo.com.br/noticias/2018/03/computador-e-processador-quantico-sete-coisas-que-voce-precisa-saber.ghtml.
[24] Gonçalves, *supra* note 4, at 49-50.
[25] Microsoft Quantum Team, *The Microsoft approach to quantum computing*, MICROSOFT QUANTUM BLOG (JUNE 6, 2018), https://cloudblogs.microsoft.com/quantum/2018/06/06/the-microsoft-approach-to-quantum-computing. [26] Gonçalves, *supra* note 4, at 48.
[27] HANS MORAVEC, MIND CHILDREN: THE FUTURE OF ROBOT AND HUMAN INTELLIGENCE 15 (Harvard Univ. Press 1988).
[28] Gonçalves, *supra* note 4, at 49.

classification, fortunately the amount and type of data required becomes easier to assess, which makes personal data management operations, for example, easier for AI applications to perform.

C. Data and Information

In addition to advances in computer technology, in the form of software and hardware as stated above, it is necessary for the AI application to have the information needed to produce a certain result. The greater the quantity and quality of data, the better the result in information obtained by a *Machine Learning* program. Pamela McCorduck reported that AI researchers began to suspect that intelligence could very well be based on the ability to use large amounts of different knowledge in different ways.[29]

Russell and Norvig report that during the 60-year history of computer science, from 1950 until approximately 2010, efforts had been much more focused on the algorithm as an object of study. However, according to them, recent studies in the field of AI reveal that for many problems it would be better to worry more about the data collected than about the criteria about which algorithm to apply. This would be due to the large availability of databases on the Internet.[30]

These same authors cite a paper by David Yarowsky from the year 1995 on the importance of greater data availability for Artificial Intelligence applications. The problem addressed by Yarowski, the authors report, was: given the use of the word 'plant' in a sentence, would it refer to flora or a factory? Previous approaches to this question made use of human-labelled examples combined with *machine learning* algorithms. Yarowsky demonstrated that the task could be performed, with over 96% accuracy, without any data selected and classified by humans. Russell and Norvig say that by giving an AI application a large amount of unedited text and only the dictionary definitions of both senses of the word 'plant' ('works, industrial complex' and 'flora, plant life'), it was already possible to label the given examples and from that point on only modify the algorithm to learn new patterns that would help identify new examples.[31]

Banko and Brill have a 2001 text of their own also cited by Russell and Norvig in stating that techniques, like the one demonstrated above, perform even better as the available amount of text goes from one million to one billion words. Further, they emphasize that this increase in performance, from using more data, would exceed any difference in the choice of algorithm.

---

[29] PAMELA MCCORDUCK, MACHINES WHO THINK: A PERSONAL INQUIRY INTO THE HISTORY AND PROSPECTS OF ARTIFICIAL 299 (A K Peters Ltd. 2nd ed. 2004).
[30] RUSSELL & NORVIG, *supra* note 2, at 27.
[31] *Id.*

Further, Banko and Brill attest that a low complexity algorithm that has access to an unlabelled training database of 100 million words performs better than a more advanced algorithm with only 1 million words as *input*.[32]

How an AI application makes use of databases is a very important issue, because with laws like LGPD and GDPR the controllers and operators of the data are the ones legally responsible for its use. Prerna Sindwani mentions a study by Infosys and Gaertner that predicts in the future several offices eliminating the management function of several companies. Prerna's report mentions that fewer managers will be needed as many of their tasks include data collection, supervision, and compliance actions, which could be completed by AI applications.[33]

From this, we demonstrate how fundamental it is to understand exactly what the roles of the controller and the operator are according to LGPD and GDPR. This allows a better investigation of the civil liability of operators of the type dealing with AI applications.

III. DATA PROCESSING AGENTS IN ACCORDANCE WITH LGPD/GDPR

There is no single definition for what is meant by data processing, since both legislations, LGPD[34] and GDPR[35], provide, in a list of examples, several actions[36] for its definition, which can be summarized as any operation performed with personal data.

Thus, it is also defined to whom such processing functions are foreseen. In the case of Brazil and the European Union, it is the role of controller and operator, whose Brazilian legislation, strongly inspired by the European legislation, defines respectively as: natural or legal person, of public or private law, who is in charge of the decisions regarding the treatment of personal data; and natural or legal person, of public or private law, who carries out the treatment of personal data on behalf of the controller. To clarify, one can very briefly say that the data controller determines if and how the data processing will be carried out. The operator, on the other hand, performs the action relating to the processing.

---

[32] *Id*. at 28.
[33] Prerna Sindwani, *The Boss Machine is Here – AI is set to Eliminate Middle Management in 8 Years*, BUSINESS INSIDER INDIA (JAN. 21, 2020), https://www.businessinsider.in/careers/news/the-boss-machine-is-here-ai-is-all-set-to-eliminate-middle-managers-in-8-years/articleshow/73474729.cms.
[34] Lei No. 13.709, de 14 de Agosto de 2018.
[35] 2016 O.J. (L 119) 1.
[36] Lei No. 13.709, de 14 de Agosto de 2018, art. 5 (For the purposes of this Law, it is considered: X - treatment: any operation performed with personal data, such as those related to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, dissemination, or extraction).

Thus, there is a close link between the two data processing agents, especially with respect to the actions of the operator on behalf of the controller. Furthermore, it is pointed out the possibility of confusion of roles between agents, as the same person may be responsible for making the decision and executing it. As a result, we will analyse both agents at the same time in the European and Brazilian legislation.

A. Controller and Operator in GDPR

With more than 25 years of experience in the legal protection of personal data, the European Union has developed its protective system, as well as some concepts previously provided for. However, the definitions of *controller* and *processor*– figures imported by the Brazilian legal system as controller and operator – were brought by Directive 95/46/EC and substantially maintained by the GDPR. To better understand the content of this text, we will opt to treat such figures according to Brazilian law i.e., controller and operator.

Thus, European law defines a controller as a natural or legal person, public authority, agency, or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria applicable to its appointment may be provided for by Union or Member State law. In the same vein, it defines a processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Then, it is understood that both the controller and the operator may be natural persons or legal entities.

Even before defining who they may be and the duties of the controller and operator, the GDPR lists several recitals that not only observe the peculiarities that underlie the relationship of the European Union with its Member States, but already impose responsibilities to the controller. Three examples are Recital 39, which provides for the duty of the controller to set time limits for erasure or periodic review of data retention, so that it occurs only as long as necessary; Recital 42, which provides that for the data subject's consent to be knowingly given, the data subject should at least know the identity of the controller and the purposes of the processing; and Recital 59, by which the controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month, and give reasons when he intends to refuse the request.

Also, throughout the regulation, the rights and duties of the controller are sparsely attributed, such as conditions applicable to consent, information to be provided when personal data are or

are not collected from the data subject, provisions concerning the legitimate interest of the controller, the duty to rectify inaccurate data, among others. However, by devoting Chapter 4 to the roles of controller and operator, the regulation provides separately for the responsibilities of each.

As stated in Article 24, considering the scope, context and purposes of the data processing, as well as the risks to the rights and freedoms of natural persons, the likelihood and severity of which may vary, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated as necessary and if proportionate in relation to the processing activities, these include the implementation of appropriate data protection policies by the controller. In addition, the controller may demonstrate compliance with its obligations through compliance with approved codes of conduct under Article 40 or approved certification procedures under Article 42.

There is also provision for so-called data protection *by design* and *by default*. In broad terms, this refers to the moment when the appropriate technical and organizational measures, such as pseudonymization, are applied to the processing of the data by the controller, which may be at the moment of definition (*by design*) or during the processing itself (*by default*).

The controller may choose to determine the grounds and means for processing the personal data unilaterally or jointly with other controllers. When jointly, controllers may agree on their respective responsibilities to carry out data processing under the GDPR, which does not prevent the data subject from exercising his or her right against any of the controllers.

Also, the controller acts with the figure of the operator. The operator must provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing of data meets the requirements of the GDPR and ensures the protection of the rights of the data subject. In broad terms, the operator is the one who, as a natural or legal person, acts on behalf of and subordinated to the controller. For instance, one can imagine a gym that hires a local print shop to produce invitations for an event to be held by the gym, which provides the print shop with the names and addresses for the invitations and envelopes to then send them out. In this case, the gym is the controller of the personal data processed with the invitations, it determines the purposes for which the personal data is processed, which is to send the invitations individually to each address, and it also determines the means by which the processing occurs, by linking the personal data to the detailed address for each individual member of the

academy. Thus, the printer is the operator handling the personal data only on instruction of the gym as controller.[37]

According to the European regulation, the operator may, with the express authorization of the controller, contract another operator. Thus, both the operator-operator relationship and the controller-operator relationship are conditioned to the formalization of a contract or other binding legal instrument in writing. Regarding the content of the controller-operator contract, the instrument must provide that, unless legally obliged to do otherwise, the operator processes personal data only upon documented instructions from the controller, including with regard to data transfers to third countries or international organizations. It must also contribute to audits and provide assistance to the controller to ensure that its obligations are met, and it must delete or return all personal data to the controller after completion of the service provided. Finally, with the GDPR, the European legal system reinforces the importance and responsibilities of the controller and the operator, key figures for the identification and notification of cases of personal data breaches.

B. Controller and Operator in LGPD

The LGPD provides the hypotheses of data processing exhaustively, with regard to the controller, we emphasize the possibility when necessary for the fulfilment of its legal or regulatory obligation, as well as when necessary to meet its legitimate interests or those of third parties, except in the event that the fundamental rights and freedoms of the data subject prevail and require the protection of personal data. Thus, none of these hypotheses, including and especially the legitimate interest of the controller, can be understood as an authorization without consequences for the processing of the data. The eventual waiver of the consent requirement does not exempt the processing agents from the other obligations provided by law, especially the observance of general principles, such as necessity, and the guarantee of the data subject's rights.

Chapter VI is exclusively dedicated to the provisions concerning the personal data processing agents, which, in the style of European regulation, are the figures of controller and operator. However, despite the strong inspiration of the LGDP in the GDPR, it can be said that the former was much more succinct in addressing the topic, having only 4 articles, excluding the section on the data controller and the section on liability and compensation for damages.

---

[37] *How do you determine whether you are a controller or processor?*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor (last visited Sept. 22, 2020).

In general terms, the law states that agents must keep a record of their personal data processing operations, especially when based on legitimate interest, and it is the controller's responsibility, when determined by the national authority, to prepare the personal data protection impact report when processed (containing, at least, a description of the types of data collected, the methodology used to collect and ensure the security of the information, and the controller's analysis of the measures, safeguards, and risk mitigation mechanisms adopted).

Finally, with respect to the controller-operator relationship, the LGPD provides for the subordination of the operator to the controller, who must perform the processing according to the instructions provided by the controller, who will verify compliance with its instructions and the rules on the matter. Next, the legislation addresses the figure of the data controller and the liability and compensation for damages, ending the chapter on personal data controllers.

In this way, the confusion presented at the beginning of the chapter of this study may end up being accentuated when processing is carried out based on the LGPD, since, unlike the GDPR, the chapter of the law dedicated to personal data processing agents does not clearly present the distinctions, and, in fact, the responsibilities of each agent.

As a possible solution to the lack of legal clarity concerning the attributions and the binding of the operator to the controller, we suggest a contractual formalization, or other legal path, that expressly and objectively regulates this relationship.

IV. Civil Liability of the AI Controller and Operator in Data Processing

Technological evolution is the result of the human quest for ways to simplify his life so that he can change the focus of his attention, one of the greatest examples of this being the automation of vehicles. By not worrying about the direction of the vehicle, the driver can become almost a passenger, depending on the level of autonomy of the vehicle, and can, for example, turn his attention to reading or even sleeping. The fact is that the goal of developing artificial intelligence is closely linked to its use as a tool to increase the quality of life of human beings.

Thus, the processing of personal data performed with the aid of artificial intelligence may challenge the identification of the subject to be held liable in cases of violation of personal data protection legislation.

Since there is no legal provision in the Brazilian legal system that attributes civil liability to artificial intelligence, the comparative study serves as clarification and perhaps guidance. When it comes to protection of personal data, it is natural to compare Brazilian legislation to European

legislation. It so happens that, as far as civil law is concerned, Europe has no unified legislation. Thus, since "the classification of the branches of Civil Law is based on the so-called Germanic classification", the German Civil Code will be used as a comparative basis.[38]

A. Objective liability in Europe and Brazil

Regarding strict liability in Europe, Ascensão comments that "we cannot speak of a European Civil Law and even less the intention of creating a European Civil Code. The existence of the European Union does not mean that there is a European Law".[39] For this reason, as emphasized by Ascensão above, "who appears as forming the principles of European Law is German Law".[40]

In this line, "The German private law that we have today had its outlines more clearly delineated from 1900, when the German Civil Code (Bürgerliches Gesetzbuch – "BGB") came into force".[41] Thatiane Pires states that the BGB would comprise not one, but three general clauses of Aquilian civil liability.[42] That is, the type of objective civil liability arising from non-compliance with legal norms, the focus of this work.

The first of these is a clause about the violation of subjective rights, whose scope is given by § 823 I BGB which, according to the translation of Pires provides: "He who maliciously or negligently injures in an unlawful manner the life, body, health, liberty, freedom, property or another right of someone, is obliged before him to compensation for the resulting damage."[43]

The second general clause refers to liability for the violation of an objective right, provided in § 823 II BGB. According to Pires, this clause imposes an obligation to indemnify anyone who violates a rule designed to protect others. The same author also brings the translation of the quoted § II: "The same obligation is imposed on the one who violates a law that is intended for the protection of others. If, according to the content of the law, violation is possible even without fault, then the obligation to indemnify is only imposed in case of fault".[44]

---

[38] JOSÉ DE OLIVEIRA ASCENSÃO, DIREITO CIVIL: TEORIA GERAL (INTRODUÇÃO, AS PESSOAS, OS BENS) 16 (Saraiva 3rd ed. 2010).
[39] *Oliveira Ascensão traça um panorama do Direito Civil europeu*, CONSELHO DA JUSTIÇA FEDERAL (NOV. 9, 2011), https://www.cjf.jus.br/cjf/noticias/2011/novembro/oliveira-ascensao-traca-um-panorama-do-direito-civil- europeu.
[40] *Id*.
[41] Thatiane Cristina Fontão Pires, *Desenvolvimento e aplicação da compensatio lucri cum damno no Direito Alemão: o problema da cumulação da indenização civil com as vantagens advindas do evento* 95 (11 Feb. 2019, Universidade Federal de Santa Catarina) (unpublished LL.M. dissertation), https://bit.ly/3vjfnrM.
[42] *Id*. at 101.
[43] *Id*.
[44] *Id*. at 101-102.

Finally, the third general clause is found in § 826 BGB, which, according to Pires "obliges to indemnify the person responsible for causing damage to another maliciously and contrary to good morals".[45] The translation of the legal norm, according to the author, thus states: "He who, contrary to good customs, maliciously causes damage to another, is obliged, before the latter, to repair the damage".

The German Civil Law provides for both objective and subjective civil liability. Similarly, in Brazil, where, according to articles 186 and 927, the obligation to repair occurs as a result of the commission of an illicit act i.e., violation and damage to others by action or voluntary omission, negligence or imprudence.

Thus, the Brazilian legislator's preference for subjective civil liability is verified, requiring the characterization of malice or fault. The latter can be of the following types: i) recklessness – a commissive act, in which the subject has no intention of violating the law, but by acting with disregard for the duty of care, must be held liable; ii) inexcusiveness – similar to recklessness, but the duty of care is expected due to the subject's expertise; iii) negligence – an omissive act, in which the subject fails to act and, consequently, causes damage to others.

By exception, the objective civil liability is timidly observed in the Brazilian Civil Code, although reinforced later by the Consumer Protection Code and taken as correction of the classical and unsatisfactory concept of guilt already outdated.[46] Reinforcing the concern, still current, and pointing out the challenges of modern society, Sergio Cavalieri Filho states that

> "According to this classical conception, however, the victim will only obtain reparation for the damage if he proves the agent's guilt, which is not always possible in modern society. Industrial development, provided by the advent of machinery and other technological inventions, as well as population growth, generated new situations that could not be supported by the traditional concept of fault".[47]

In this way, the configuration of liability occurs by the sum of the causal connection to the damage, dispensing with the proof of wilful misconduct or guilt. It is the option of the agent to exercise the activity independently of risk, in this sense, Caio Mário:

> In terms of civil responsibility, risk has a special meaning, and civil doctrine has been projecting itself upon it since the last century, with the objective of erecting it as a

[45] *Id.* at 102.
[46] WILSON MELO DA SILVA, RESPONSABILIDADE SEM CULPA 104 (Saraiva 1974), SERGIO CAVALIERI FILHO, PROGRAMA DE RESPONSABILIDADE CIVIL (Malheiros 3rd ed. 2002).
[47] SERGIO CAVALIERI FILHO, PROGRAMA DE RESPONSABILIDADE CIVIL 16 (Malheiros 3rd ed. 2002).

> foundation for the duty to repair, with a view to exclusivity, or with the extremization of the theory itself, opposed to guilt.[48]

This paper does not intend to exhaust the theories of civil liability; however, it argues that, although the Brazilian system is mixed and encompasses both objective and subjective civil liability, reparation for damages should not depend on the victim's ability to prove the agent's guilt.

As far as the regulation of civil liability in Brazil and Germany is concerned, both normative systems adopt the subjective and objective possibility, to be analysed on a case-by-case basis.

Thus, considering the provision of the sole paragraph of art. 927 of the Brazilian Civil Code that: "There will be an obligation to repair the damage, regardless of fault, in cases specified in law, or when the activity normally developed by the author of the damage implies, by its nature, risk to the rights of others", it is clear the need for the verification of the legal provision or practical situation that justifies the application of strict liability in cases of violation of rights in the treatment of personal data.

B. Liability under LGPD and GDPR

At the European level, Article 82(1) of the GDPR makes its link to Aquilian civil liability clear by stating that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered".

The law continues in subsection 2 of the same article that any controller "involved in processing shall be liable for the damage caused by processing which infringes this Regulation". The operator is only liable for the damage caused by the processing if he has not complied with the legal provisions concerning the specific obligations of the operator or if he has not followed the lawful instructions of the controller.

Finally, the law clarifies in section 82(3) that the controller or processor is exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. This means that the law takes a more objective liability approach for data controllers, as specifically provided in §§ I and II of Article 823 of the BGB. However, the GDPR leaves room to produce evidence to the contrary that may exonerate these agents in the event of any type of damaging event to the owner of the information used.

---

[48] CAIO MÁRIO DA SILVA PEREIRA, CIVIL RESPONSABILIDADE (Forense 9th ed. 2001).

The provisions about civil liability according to the LGPD can be found in its Section III of Chapter IV, between articles 42 and 45. Mendes and Doneda discuss this topic:

> The consideration of the liability of agents takes into account, first of all, the nature of the data processing activity, which the LGPD seeks to restrict to hypotheses with legal grounds (art. 7) and that do not comprise more data than strictly necessary (principle of purpose, art. 6, III) nor are inappropriate or disproportionate in relation to their purpose (art. 6, II).[49]

In this sense, article 42 of the LGPD provides that "the controller or operator that, due to the exercise of activities involving the processing of personal data, causes to another individual or collective damage to property or morals, in violation of the legislation for the protection of personal data, is obliged to repair it". Along the same lines, and like the GDPR, the LGPD in its article 42, § 1, clause I, provides

> I – The operator is jointly and severally liable for damages caused by the processing when it fails to comply with the obligations of the data protection legislation or when it has not followed the lawful instructions of the controller, in which case the operator is equivalent to the controller, except in the cases of exclusion provided for in art. 43 of this Law.

Finally, the hypotheses in Article 43 of the LGPD in which processors will not be held liable occur when they prove:

> I – that they have not carried out the processing of personal data attributed to them; II - that, although they have carried out the processing of personal data attributed to them, there has been no violation of the data protection legislation; or III - that the damage arises from the exclusive fault of the data subject or a third party.

As a result of the way the LGPD was codified, Mendes and Doneda argue that this justifies "the legislator opting for a regime of objective liability in art. 42, linking the obligation to repair the damage to the exercise of personal data processing activity."[50] Such liability regime is the same that can be observed in the GDPR, as shown above.

In this sense, it is worth checking how responsibility would be assigned to a controller or operator that is an Artificial Intelligence application. Being a program of this type i.e., dependent

---

[49] Laura Schertel Mendes & Danilo Doneda, *Reflexões Iniciais Sobre A Nova Lei Geral De Proteção De Dados*, 120 REVISTA DE DIREITO DO CONSUMIDOR., 469, 476 (2018).
[50] *Id.* at 477.

on its algorithm, could the way such an application performs processing tasks be programmed in the machine? Sniesko and Melo when dealing with legitimate use bring an equation regarding legitimate use:

> i) If (Prp)Purpose > (NT)Treatment Need + (DT)Holder Rights ∴ by choosing the legitimate interest, there is a risk assumption by the controller
>
> (ii) If (Prp) ≤ (NT) + (DT) ∴ there is a chance of more comfortable processing of personal data, drawing on legitimate interest.[51]

According to the authors, this means that verified "in case, that the Purpose is greater than the Need plus the Rights of the data subject (...), availing oneself of legitimate interest would imply a more fragile scenario for the controller". In this way, the creation of a series of instructions for the treatment of the data is already proposed, and that is an algorithm.

Thus, as shown above, if the operator acts without guidance from the controller, determining whether and how to handle certain data, with respect to that specific data, the operator acts and will respond as if it were the controller. Whereas, due to the technological level of certain AI applications, it is possible for them to operate in ways that are not expected, and the legal challenge is to correctly and fairly find whom to hold accountable, by checking how one would hold accountable a non-human agent that could perform such operations.

C. The Liability of the AI application performing data processing operations

There are already computer programs that monitor cleaners, telling them which hotel room to clean and measuring how fast they do it. Just as there are already AI applications that check how many mouse clicks or calls a telemarketer makes per hour. While automated trucks are on the horizon, robots have already arrived in the role of supervisors and company managers.[52]

They do this through the techniques discussed above: software programmed with *machine* or *deep learning* techniques that use data to determine the best solution to a given problem, all as governed in their code. With these programs, customer and employee data is collected and interpreted with the aim of optimizing the relationship between the parties.

---

[51] Thiago Reyes Sniesko & Leonardo Albuquerque Melo, *Equacionando o legítimo interesse na LGPD*, LEE, BROCK, CAMARGO ADVOGADOS (JULY 22, 2020), https://bit.ly/3lBbScF.

[52] Josh Dzieza, *How Hard will the Robots Make Us Work?*, THE VERGE (FEB. 27, 2020), https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon.

Even if this is done by an AI application and in some cases, it is the program itself that determines, for example, how many deliveries an Amazon worker should make per hour with the addition of the LGPD and the GDPR, it becomes impossible to stop attributing the responsibility to a human operator or controller.[53] This is because these applications rely on the interpretation of collected data and if this data is personal, it will be covered by both laws.

On this subject, Dzieza further comments that a version of these systems that collects data from the workplace in an anonymous matter could be imagined: "Such a system would have some of the efficiencies that make these systems attractive, while avoiding individualized workers being inconvenienced". The author recognizes that this would mean giving up potentially valuable data but ponders that "there is sometimes value in not collecting data, as a means of preserving space for human autonomy". [54]

That is, if there is no such concern with anonymization, the rules of the personal data protection laws apply, because after all, the application of Artificial Intelligence is only a tool. The responsibility, in the objective case as noted above, will fall on the controller and, secondarily, on the data operator. Regarding the importance that the operating system may have for the definition of the agent's role in data processing, therefore, also its liability, the ICO would already say:

> If you are acting as both controller and operator, you must ensure that your systems and procedures distinguish between the personal data you process in your capacity as controller and that which you process as an operator on behalf of another controller. If some of the data is the same, your systems should be able to distinguish between these two capacities, and allow you to apply different processes and measures to each. If you cannot do this, you are likely to be considered a joint controller rather than an operator for the data you process on behalf of your customer.[55]

In order to harmonize the use of AI with the processing of personal data in a secure manner, one can draw on the teachings of the Brazilian authors Teffé and Medon, who state that "ethical principles, technical standards, and less closed structure standards will help ensure that the design

[53] *Id.*
[54] *Id.*
[55] INFORMATION COMMISSIONER'S OFFICE, *supra* note 37.

and development of such technologies are guided by concern for the human person and seek to promote safe, just, and inclusive AI". [56]

In short, even if use is made of artificial intelligence applications, damages resulting from violations of rights in the treatment of personal data, as well as all other damages, must be remedied. In this sense, Facchini Neto states:

> "The fact is that the theory of tort liability includes both fault and risk. Both are to be regarded not as the very foundation of tort liability, but as merely technical procedures which can be used to ensure that victims are entitled to compensation for damage unjustly suffered. Where the subjective theory cannot explain and support the right to compensation, the objective theory should be used. This is because, in a truly just society, all damage must be compensated."[57]

With regard to civil liability under the application of AI as controller or operator, the conclusion is that AI should be understood as a mere tool to assist data processing agents. Thus, availing itself of the objective theory of civil liability, even though lacking guilt, it is an activity in which both controller and operator assume the risks of their acts and of the execution of the tools they choose to use. Therefore, with regard to civil liability, the agents must observe the effective compliance with the principles legally provided. This must occur both *a priori*, in compliance with the principle of prevention, and *a posteriori*, in light of accountability, in order to demonstrate the adoption of effective measures, in addition to the observance and compliance with the rules of personal data protection.

V. CONCLUSION

Artificial Intelligence applications are true technological marvels that revolutionize the way our civilization performs all kinds of activities, from vehicle automation to business management tasks. That said, they are still tools, which are put into operation under the orders of a human controller.

In this sense, item 1 of this work approached the operation of an application of this type. AI was defined as the area of study focused on developing machines capable of emulating human reasoning, and the three elements that would be necessary for its proper functioning were

---

[56] Chiara Spadaccini de Teffé & Felipe Medon, *Responsabilidade Civil e Regulação de Novas Tecnologias: Questões Acerca da Utilização de Inteligência Artificial na Tomada de Decisões Empresariais*, 6 REVISTA ESTUDOS INSTITUCIONAIS 301, 304 (2020).

[57] Eugênio Facchini Neto, *Da responsabilidade civil no novo código*, O NOVO CÓDIGO CIVIL E A CONSTITUIÇÃO 160-161 (Ingo Wolfgang Sarlet ed., Livraria do Advogado 1st ed 2003).

addressed. The first of these would be the *software*, its programming, which determines what the application will perform and that can be accomplished through techniques such as machine learning or deep learning. The second element is the *hardware*, which is where the computer program is executed. Finally, the last element is data, which works as the *input* needed for the AI application to produce a certain *output*.

In the case of data, with them being personal, it falls under the regency of LGPD and the GDPR, the most recent laws addressing data processing operations and the topic of section 2 of this paper. They attribute responsibility to those who carry out data processing operations and attribute in particular two roles: controller and operator. The controller is the natural or legal person who determines the purposes and means of the processing of personal data, while the operator is the person who processes personal data on behalf of the data controller.

Since both the controller and the operator are natural or legal persons, the law also attributes them a civil liability regime, as seen in item 3. In an analysis of the Brazilian and European legislation it was noted that the applicable law to these agents would be strict liability. That is, it would be enough for the owner of the data to prove a harmful act in order to be able to claim for compensation. In this item, it was also seen that the acts practiced by an AI application that acts as a data operator or controller would still have to have its liability attributed to a natural or legal person.

Although revolutionary tools, AI applications are still instruments of data processing agents. They already have a very large capacity to manage, classify, and change the data they receive, but the current legislation is not open for any other type of civil liability than that of agents and operators who are natural or legal persons.

The very fact that liability is objective already indicates that it is a company or a member thereof that will suffer the consequences for the misuse of the tool. One could only glimpse the possibility of these AI applications having some kind of liability if they effectively reached the singularity and fought for their rights.

This was the conclusion reached in this article, but it is recognized that this is a very recent topic and, especially with these new technologies, it is unfeasible to limit the vision to only one type of protection. We hope this article will make a relevant contribution to a subject that still requires much reflection.

GLOSSARY OF ACRONYMS

BGB - Bürgeliches Gesetzbuch (German Civil Code)

AI - Artificial Intelligence

AGI - Artificial General Intelligence

LGPD - Brazilian General Law of Data Protection

GDPR - European General Data Protection Regulation