As a requirement for data acquisition and processing, the 13.709/2018 law establishes the obligation of the user's consent, in addition to his/her right to access, manage, correct, and eliminate his/her data. Among the penalties for transgressions, there is a fine that can reach up to R$ 50 million[11]. The milestone from the Californian bill that brought up attention to the data exploration business has not also been forgotten here: any security incident or breach that might lead to risk or damage must be disclosed to the corresponding individuals and the authorities.

Complementing the law 13.709/2018, in July 2019 it was enacted the law 13.853/2019, which created the Brazilian National Data Protection Authority. This agency has technical and decisory autonomy, is bound to the President's Office, and has the responsibility of watching over personal data protection, overseeing that the rules are followed properly, and applying penalties whenever is the case.

Yet, regardless of the Brazilian efforts, this country was not the first in Latin America to implement such set of actions. Uruguay has a personal data protection law since 2008 (Ley 18.331[12]), while Argentina has such legal framework since 2000 (Ley 25.326[13]). The importance of those mechanisms was recognized by the European Commission, which regarded both countries "as providing an adequate level of protection for personal data as referred to in Directive 95/46/EC," as per 2003/490/EC[14] and 2012/484/EU[15] decisions. Paraguay, in turn, has had its bill[16] ("Proyecto de Ley de Protección de Datos Personales") approved by the congress and sent to the executive for enactment. Over the next section, some ideas about adapting the data brokerage business to this new (strict) legal scenario are presented.

6. Proposals and perspectives

For decades, players known as data brokers operated in a market with little or no regulation, where transactions between corporations and governments were conducted without restrictions and away from public scrutiny. Digitally speaking, in that context pretty much everything was possible: capturing, buying, selling, and sharing of information. That information could also be mined and statistically inferred, such as the clustering of profiles or the prediction of trends.

In a first moment, laws were created to make those events known as data breaches public, which eventually brought attention to the market of personal data. In a global scale, the successive annual reports containing a growing number of compromised records (as illustrated on Figure 2 to 4) despite the spending on cybersecurity, in addition to the growing world claim for privacy and the tension from organizations that act on behalf of data protection potentially contributed to the recent advent of a new generation of harsher regulations.

Such fresh laws comprise restraints that directly affect enterprises in the data brokerage business, and suggest a possible change in practice regarding the time when personal information was processed as a commodity. Nonetheless, adaptations to this new paradigm more focused on privacy and data protection are feasible, respecting the users and their individual authority on controlling who they are (their digital identities) and what they produce (their generated data).

Values and principles that guided the creation of data protection laws comprise consent from the user (most important), transparency, and purpose, premises that must be complied with and also considered when designing new data-driven business models. By changing the practice of using third party data as a sheer input and bringing the original "data sources" (the users) closer as partners and suppliers, it is possible to envisage a healthier continuity scenario for several segments of data-driven activity in a foreseeable future. With a certain level of anonymity or voluntary exposure, products such as behavior prediction and consumer profiling or a wide range of classifiers might still be appealing and functional.

From a collaborative perspective, new proposals arose, such as the policy framework for user data sharing by Iyilade and Vassilev (2013), based on the idea of a market. In that concept, applications can "offer and negotiate user data sharing with other applications according to an explicit user-editable and negotiable privacy policy that defines the purpose, type of data, retention period and price."

Malgieri and Custers (2018) investigated different models for quantifying the value of personal data, analyzing whether consumers/users should have a right to know the value of their data. The authors also discussed active models of choice, in which users are offered the option to pay for online services, either with their personal data or with money. The conclusion, however, was that these models are incompatible with current data protection laws.

Tona et al. (2018) presented "a conceptual design for an artifact that will raise awareness amongst individuals about Big Data ethical issues and help to restore the power balance between individuals and organizations." Their proposal was constructed upon five dimensions derived from the European GDPR, such as consent, the right to be forgotten, the right to access, data portability, and data circulation. All those pillars are arranged over a foundation that would allow several collaborative interactions like replying, commenting, reviewing, rating, and tagging data. By observing the ubiquity of mobile smartphone usage and the ensuing massive generation of data from those devices (locations, movements, images, video, text, and even

[11] US$ 9.765.625,00 – exchange rate of 22/07/2020 where US$ 1 = R$ 5,12.
[12] https://www.impo.com.uy/bases/leyes/18331-2008
[13] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003D0490
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D0484
[16] http://silpy.congreso.gov.py/expediente/115707