Centre for Information Policy Leadership
Hunton & Williams LLP

5 April 2017 (1 June 2017)

DISCUSSION POINTS
BRAZIL PROPOSED DATA PROTECTION LEGISLATION
5276/2016 – MINISTRY BILL

The following points are CIPL's comments on certain key issues relating to Brazil's draft Ministry bill 5276/2016. Our comments are based on English translations of the text. It is possible that, as a result, we may have misunderstood some particular intent or nuance on a particular issue, in which case, please disregard our comment on that issue.

1. General comments

CIPL welcome the recognition in Article 2 that this data privacy law is not only based on the need to protect individuals privacy but must also be consistent with freedom of expression, economic and technological development and free enterprise and competition.

CIPL also believes that the current draft includes several significant improvements over earlier drafts. For example, we welcome the inclusion of the "legitimate interest" ground of processing, the inclusion of risk assessment and, thus, a risk-based approach in the provision on "good practices", a broad range of cross-border transfer mechanisms, and the provision for a "competent body," among other items.

Over the past few years, a global "data and digital revolution" has drastically changed the landscape to which data privacy laws apply. We now live in a new "digital age" that is based on and driven by big data, the Internet of Things (IoT), Artificial Intelligence (AI) and machine learning. Everything is data and data is everywhere. Data flows around the globe in ever-increasing quantity and is used in ever increasing and complex ways. This presents a new reality that has to be taken into account when devising new privacy and data protection laws that are fit for the new information age. Brazil currently has a unique opportunity to create a law that can meet the needs of this digital age, taking into account the experiences, mistakes and successes of other privacy regimes around the world. Most if not all of these legacy privacy regimes were devised prior to the digital age and are now also faced with the need to modernize.

In that connection, it is important to avoid creating laws that will become obsolete with the next technological advancement or whose total impact is not fully understood at the time of drafting and that, therefore, may have unintended consequences for legitimate and beneficial data uses. Naturally, it is the organisations who will have to comply with these provisions that are in the best position to foresee such potential consequences. Thus, we strongly recommend that as part of multistakeholder consultations, these organisations be extensively consulted on the details of any final provisions.

To be able to meet the demands of this new digital age and be future -proof, we believe that a data privacy law for Brazil must have the following key characteristics:

1. **Be clear and easy to understand, apply and enforce**. This law has a wide scope of application and would apply to all personal data (of citizens, customers, employees, business contacts) and cover all industry sectors and commercial enterprises of all sizes,

including sectors with no data protection experience and small businesses with no expertise or ability to hire data protection officers to help them comply. It is essential that the requirements be simple, easy to comprehend and implement across the board.

2. **Follow a principles-based approach:** Rather than include too many specific and detailed requirements, high-level principles and "goals" will allow organisations to apply these principles flexibly with the help of appropriate benefits/risk analyses that will determine the specific appropriate data protection measures for a given context, particularly as technology and business practices change and individuals' expectations evolve.

3. **Include a risk-based approach:** This means that organisations should be required to understand the risks and harms to individuals of any data processing and data use, as well as benefits of processing, and are able to calibrate compliance based on potential risks and harms. In that way, they can concentrate their compliance efforts, mitigation actions and accountability (good practices) on areas that may cause risks and harms. Equally, they should not spend too much effort on areas that do not create risks and harms to individuals, such as in the B2B data processing context, or other common and everyday uses of data.

4. **Remain technologically neutral:** (e.g., on issues such as data security) so that the law can adapt to technological changes and remain relevant.

5. **Provide for varied legal basis for processing and data transfers:** The law should include a range of grounds for processing, ranging from consent to legitimate interest, each of which can be applied pragmatically in appropriate contexts to enable the full range of beneficial data uses in the modern information age while also protecting the individual. The law must also provide for a broad range of cross-border transfer mechanisms that mirror and are able to work with all other international transfer mechanisms to enable the seamless flow of data around the globe that is essential both to a modern economy and the use of data for commercial purposes and for societal progress.

We believe that much of this is already accomplished by the current draft. However, the more detailed comments below on some of the key provisions in the draft may further improve this law consistent with these high-level concepts.

2. Purpose of data protection law (Article 2)

Overarching message: Is it helpful and appropriate for data privacy law to reflect additional and sometimes competing interests and values that must be taken into account and balanced when protecting personal privacy, such as enabling innovation, economic development and societal advancement.

- We welcome the recognition that data privacy laws must not only enable privacy protections but also other values, including innovation and responsible use of data for economic, societal and technological development.

- Equally, data protection authorities today have the **dual role** of privacy protection on the one hand and enabling the responsible use of data in modern data economy and society on the other.

3. Controller/Processor Distinction and Jurisdiction (Article 3)

Controller/Processor Distinction

Overarching message: We encourage clarification of the distinction between controllers and processors (operators) throughout the text of the legislation, as their roles and responsibilities for data protection differ.

- As a general matter, the draft law appears to recognize that data controllers are the entities that collect and use data about individuals for various purposes, make all decisions regarding data processing and may engage third party-data processors to perform various functions on their behalf. It appears that the draft recognizes that controllers are the entities that should be responsible for complying with data privacy laws.

- While third-party processors are not explicitly referenced, the text appropriately implies that the third-party processors only act on the controllers' behalf and are merely implementing any legal requirements pursuant to the controller's instructions and contract.

- However, we are concerned that this distinction may not be explicitly stated or consistently reflected throughout the text. CIPL believes that the draft would benefit by including this distinction in Chapter I Article 3, where the scope of the law is defined, and in Article 6 which defines the principles of data processing. As drafted, these provisions appear to apply equally to both controllers and processors in Brazil.

- We encourage clarification of the distinction between controllers and processors and their respective roles throughout the text of the legislation.

Scope of Jurisdiction

Overarching message: The statement of jurisdiction should make clear that Brazilian privacy law does not apply to the processing of foreign data by Brazilian processors on behalf of foreign/non-Brazilian controllers. In general, the law should apply to organisations (controllers or processors) established in Brazil, irrespective of where they process the data. Further, processing of personal data of Brazilians who make online purchases from non-Brazilian domains/websites (e.g. .com rather than .br), should not be subject to this law.

- Generally, it is positive that the scope of jurisdiction has been appropriately narrowed to more closely reflect customary jurisdiction provisions found in data privacy laws globally.

- We, however, remain concerned that the scope of jurisdiction may be too broad in that Art. 3(1) would cover foreign controllers and Brazilian processors processing acting on behalf of foreign controllers. In such cases, individuals' data could be subject to foreign processing requirements that may conflict or overlap. Optimally, individuals should enjoy the protection of the law of their jurisdiction and data processors should be made responsible for treating data accordingly.

- If Brazilian law were to apply to foreign controllers and data, this would disadvantage Brazil-based processors and the IT services industry.

- However, we believe that the legislation should explicitly state with respect to the Good Practice requirements, this law also applies to processors and processing operations within the national territory. (We discuss this further in the section below on Good Practices.)

- Finally, we also believe that foreign controllers generally should not be subject to Brazil's privacy law if Brazilian consumers purchase goods from non-Brazilian domains/websites such as .com (rather than .br).

4. Consent – Sensitive Data (Article 11)

Overarching message*:* Care must be taken to ensure that consent provisions related to sensitive data not become so restrictive that they preclude the use of that data – with appropriate safeguards – for beneficial uses.

- CIPL is concerned that the consent provisions related to sensitive data may be too restrictive and not reflect the realities of contemporary data use.

- Requiring express consent for sensitive data processing will preclude a large number of beneficial uses of data (including uses that have not only commercial value but would benefit society), where the controller is not in a position to obtain consent or where consent is denied for now good reason in cases where there is no harm, for example. Thus, we encourage allowing the legitimate interest basis for processing sensitive data. Because legitimate interest requires risk assessment as well as appropriate mitigations, it will be even more protective of the personal data than express consent can be.

- We are further concerned that the research exemption may be too narrow, as it excludes research that is "associated" with commercial activities. Currently, a great deal of research that benefits society is conducted by commercial entities. Organisations should be able to use sensitive data responsibly both for commercial purposes and broader purposes that benefit society if the data is handled accountably and the is no or very low risk of harm.

- Still on this issue, we would like to call attention to the legislative proposal contained in Bill 6291/2016, which is under analysis together with Bill 5276. Bill 6291 seeks to modify Marco Civil da Internet by proposing a broad definition of personal data (mixing it with examples of sensitive data), as well as by providing for a general rule of non-sharing of data, except when sharing is carried out after the "free, unambiguous, informed and specific consent" from the data owner. CIPL believes that this legislative proposal does not reflect the current reality of data processing and has the potential to inhibit beneficial uses and sharing of personal and sensitive data. We therefore believe that PL 6291/2016 should be rejected in its entirety.

5. Consent and Legitimate Interest (Articles 5 and 7)

Overarching message on legitimate interest: CIPL is encouraged by the inclusion of legitimate interests as a legal basis for processing of data. While consent remains an important basis for data processing, increasingly not all data processing can or should be based on consent. The realities of analytic processing of big data is a critical example.

- **Overarching message on consent:** With respect to consent, CIPL believes that in cases where "express" consent is not required (i.e., with respect to non-sensitive data), that should mean opt-out consent and implied consent should be possible to ensure individuals are not over-burdened by the constant consent requirements in the digital world.

- Legitimate interest-based processing is often a more "accountable" basis for processing and better able to protect individuals than consent because it requires a balancing of benefits and risks as well as implementing appropriate mitigations.

- Article 9 states that the legitimate interest must consider the "reasonable expectations" of the individual. This provision unnecessarily restricts the application of legitimate interest, which may be particularly useful where the processing relates to new, previously unknown beneficial data uses.

- The use of publicly accessible data should not be subject to the processing requirements of Article 7.

- We suggest the drafters revisit the consent provision to make it clear that consent is not necessary when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed. For example, mobile phone data or data about neighborhoods or places of residence might be used by a public authority or authorized third party for use in disaster relief.

6. Principles, Purpose Specification and Compatibility (Article 6)

Overarching message: With respect to the "purpose" provision, we suggest expanding the scope of "purposes of which the data subject is informed" to include what is reasonably expected by the data

subject.

- "Informed" appears to impose a specific duty on the data controller; in many cases the individual may reasonably expect data to be used in certain ways as a matter of normal business practice or societal norms.

- With respect to the "adequacy provision", we believe it may be helpful to provide additional guidance about how "compatibility" is determined. It might be useful to include a provision that controllers take into account:

    - Any link between the original purposes sought and the purposes of intended further processing
    - The context in which data have been collected and processed
    - The nature of the personal data
    - Any impact of further processing on the data subject, including the likelihood and severity of harm to data subjects; and
    - The existence of appropriate safeguards.

  If the purpose of further processing is not compatible, further processing must be in accordance with the provisions in Article 7, such as consent or legitimate interests.

7. Anonymous Data (Articles 5 and 13)

Overarching message: CIPL welcomes that the draft legislation continues to acknowledge the significance of anonymized data. The legislation will best serve the data protection interests of Brazilians if it provides organisations with incentives to de-identify or anonymize data.

- We believe that anonymized data should be excluded from application of the law where re-identification is only achievable through "extraordinary" efforts. Even where re-identification could occur through mere "reasonable" efforts, the data should still be deemed anonymous and outside the law if the anonymisation is coupled with procedural and administrative protections, such as contractual and regulatory prohibitions to re-identify data except in specified circumstances. We recommend stating this explicitly in Article 4.

8. Cross-border Data Transfers/International Transfers of Data (Articles 33, 34)

Overarching message: CIPL welcomes the draft law's approach to cross-border data transfers to the extent it provides for a broad spectrum of mechanisms that can be used to legitimate transfers of personal data to countries that do not have similar levels of data protection and to the extent these mechanisms can work together with similar mechanisms in other countries.

- We welcome the incorporation of the widely-accepted concepts of "standard contractual clauses" and "global corporate standards" or "global corporate rules" (known in Europe as "Binding Corporate Rules" or "BCR.") This positions Brazil for data transfers with Europe and

other countries that recognize these cross-border transfer mechanisms.

- However, standard contractual clauses and binding corporate rules have their limitations – the former are not flexible and can result in undue complexity and the latter are limited to transfers within a corporate group and lack scalability, as they need to be approved by the competent body. (After the new EU General Data Protection Regulation (GDPR) takes effect, BCR possibly may also be used across and between corporate groups.)

- Therefore, while we encourage Brazil to include these options as legitimate mechanisms for international data transfers, we also encourage Brazil to work with experts experienced in these mechanism, including CIPL, to improve on these mechanisms and to make them up-to-date, more practical and scalable for widespread use by companies of all sizes.

- Moreover, given that modern data flows and economic activity are global, it is important to include in the menu of choices additional cross-border transfer mechanism that mirror those that are available in other jurisdictions and regions and that extend beyond intra-company transfers. Thus, we would encourage inclusion of additional mechanisms such cross-border privacy rules such as the APEC Cross-Border Privacy Rules (CBPR) and other certifications, privacy marks and seals (such as EU GDPR certifications to be developed under the GDPR), and other organizational codes of conduct that are certified by appropriate third parties or the competent authority.

- Indeed, with respect to the requirement in the draft that the "competent body" authorize these global corporate standards or rules, we suggest that this requirement be modified to allow recognized certification bodies to authorize such standards or rules, similar to the role of Accountability Agents in the APEC CBPR system to avoid approval bottlenecks within this competent body.

- It is worth noting that APEC and the EU have begun to explore ways to streamline the CBPR/BCR certification and approval processes where companies seek "dual certification" under both systems. They are also exploring how to make the new EU GDPR Certifications compatible and interoperable with the CBPR. Thus, CIPL recommends that any Brazilian counterparts to these mechanisms be designed so that they too are "interoperable" with these and other similar cross-border transfer schemes to ensure that companies that have certified, or received approval under a non-Brazilian scheme can leverage that approval in Brazil and vice versa.

9. Data Breach Notification (Articles 47 and 48)

Overarching message: CIPL welcomes the approach in the draft bill to notification of the breach to the competent authority and/or individuals, requiring such notification only with a "reasonable time" after sufficient facts about the incident have been established and when the breach may lead to material risk or damage to individual.

- The draft laws allows the *competent body* to define a "reasonable time" within which the controller must report an incident that leads to material risk and damage for data subjects to the competent body. CIPL welcomes this approach, noting that the list of items to include in the notification demonstrates the recognition by the drafters that companies need time to establish the facts and nature of the breach, what data has been implicated, and what impact, risks and harms can arise from the breach as well as mitigation measures that have been or will be taken. It takes time to undertake such forensic and legal analysis and there is no point notifying and burdening people and authorities until and unless facts are known and the risks and potential harms are assessed. In addition, in some circumstances it is important not to disclose to individuals and publicly that a breach as occurred pending a non-public criminal or other type of investigation.

- With respect to notifying individuals, the draft law provides that individuals shall be "promptly" notified regardless of whether the competent authority orders it "where there is a possibility of the incident endangering the personal safety of data subjects or causing them harm." This, too, implies a reasonable period during which the organization may establish that possibility, i.e., the nature and possible risk or harm, which is appropriate.

- Encryption appears not to be an exception under the draft. Hence even where the data or a device was encrypted the breach may have to be notified. There should be a higher bar for triggering a breach notification requirement for encrypted data. If the risk assessment after the breach concludes that the data was sufficiently encrypted and that there is no risk to individuals, there should be no requirement to notify the authority or individuals.

- Requirements that companies should disclose the nature of the security measures taken should be either eliminated or significantly narrowed to include only the general nature of the security measures taken. Disclosing too much information about security can compromise the efforts of professionals to remediate breaches and unnecessarily expose systems to future compromise by bad actors.

10. Security (Article 49)

Overarching message: Specific security requirements cannot be set by legislation, but must remain future-proof, flexible and context-specific. Organisations should determine appropriate security measures based on standards, state of the art measures, cost, nature of the data and the risks involved.

- It is counterproductive to require that security measures be determined by laws or regulations, which immediately makes them outdated, given that the laws lag behind the technology and the development of technical standards. Determination of specific security measures is best left to organisations based on standards, state of the art, cost of measures, the sensitivity of data, and risks.

- It is best for data privacy laws to include a general security requirement to implement appropriate measures to protect data from loss, destruction, unauthorised access and other

forms of unlawful processing (like in the EU GDPR). This leaves it to the organisations to determine what are appropriate measures to protect data from unauthorized access, loss, destruction, disclosures and processing in any given context, based on criteria mentioned above.

11. Good Practices (Article 50)

Overarching message: CIPL welcomes this provision, which incorporates the concepts of risk and benefits assessment with respect to data processing, organizational accountability (i.e. comprehensive corporate privacy programs) and organizational or industry codes of conduct. There should be clear incentives for organisations, both controllers and processors, that adopt privacy management programs and good practices.

- We believe that the examples of such "good practices" should also include complaint handling procedures. To avoid overburdening the competent authority and/or the courts, it is important (and possible) that most complaints by individuals be addressed initially at the company level.

- In addition to considering the risk to individuals from a data processing, risk assessments should also take into account the potential benefits. This may be encompassed by the "purpose" of the processing, but it would be preferable to mention "benefits" explicitly.

- It should also be emphasized that while data processing may raise risks, in many cases appropriate steps can be taken to mitigate them, so that the benefits of data processing can be realized. We encourage the incorporation of language that reflects *risk mitigation* as a good practice that is part of risk assessment.

- The provision should establish incentives for companies to formulate or adopt such good practice rules, such as the ability to engage in more data processing, or to be able to share data, or as a mitigation in oversight and enforcement by a competent body. For example, in the case of an enforcement proceeding, companies that adopt and adhere to such rules, and can demonstrate good faith efforts to comply, might be subject to reduced penalties in the event of a violation. This is already a recognized practice with many data protection and enforcement authorities in different countries. (This could be addressed in the section regarding "Administrative Penalties.")

- The provision should clarify that these "good practice rules" could also serve as recognized mechanisms for cross-border data transfers , as described above in section 8. (See for example the EU GDPR's use of certifications and codes of conduct as transfer mechanisms.) Thus, we suggest that good practice rules could also include adoption of certification, marks and seals. We further suggest that good practice rules could also involve adherence to recognized industry codes of conduct. Both would promote domestic compliance, but in addition could serve as mechanisms to facilitate cross-border transfer of data.

- To the extent that rules, certification or codes of conduct are intended to serve as cross-border data transfer mechanisms, they should be devised in a way that allows them to be substantively

and procedurally interoperable with similar schemes in other countries to enable cross-border solutions for companies and avoid constant re-certification of companies under similar standards.

- The text should explicitly state that the good practice rules apply to both controllers and processors, as both would benefit from implementing proactive privacy and security management programs.

12. Competent Body (Article 53)

Overarching message: We are encouraged by the incorporation of a provision that describes in detail the "competent body" that is referenced elsewhere in the bill. An independent authority will be critical to the successful implementation and enforcement of the law. It will give Brazil one centralized "expert" authority. Its mission will be to stay up-to-date on the development of technology, relevant business practices, privacy concerns, and the measures that can practically and effectively address them; to provide competent and consistent guidance and interpret and enforce the law consistently; to support and facilitate the nation's digital literacy and educate organisations and individuals about their respective rights and obligations; and to represent Brazil with "one voice" in any cross-border privacy enforcement, international privacy policy development and in the context of cooperation with foreign counterpart privacy authorities individually and through various global privacy policy and enforcement networks, such as the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and the Global Privacy Enforcement Network (GDPR), among others.

- With respect to clause VI, we suggest that the language "that facilitate data subjects' control over their personal data" be changed to "That facilitate the protection of personal data." In response to emerging technologies and data processing capabilities, privacy protection measures focus less and less on "control" and increasingly on ensuring that data is safe, protected, handled "accountably", and not used in a way that will harm them. The language we propose here would apply more broadly and would still encompass facilitating control where it is appropriate, desirable and possible.

- With respect to clause VIII, we suggest that appropriate transparency and disclosure greatly depends on context and do not lend themselves easily to regulation. Instead, we suggest the section be deleted and replaced with language to the effect of "fostering and encouraging effective means of transparency and disclosures regarding data handling operations".

- Finally, we suggest that a clause be added to this provision that enables ongoing consultations and dialogue between the authority and the regulated organisations and other stakeholders, including on issues of appropriate interpretation and implementation of the law, as well as emerging technology.

13. Timeframe for Adoption (Article 56)

Overarching message: We urge Brazil to significantly extend the 180-day time frame to allow companies sufficient time to come into compliance with the new law.

- To do this, companies will need to become familiar with the provisions of the law, understand how it may be interpreted by regulators and practically applied, and take appropriate measures internally. This is particularly important where no previous comprehensive privacy law has existed.

- A reasonable timeframe would be at least three years. The EU GDPR provides for two years, and we can already see one year into the implementation phase that organisations will not be completely ready by May 2018.

14. Effectiveness

Overarching message: We strongly recommend that this law be clarified to have prospective rather than retroactive application to personal data that has been collected prior to its effective date.

- Experience shows that it takes a long time to ensure that old legacy IT systems and existing uses of data are fully brought in compliance with new rules. As organisations struggle to apply the new requirements to existing data and processing, they lose important time to ensure their new systems, data processing and technologies comply with the law.

- Instead of retroactive application of the law, it may be helpful to state that the existing data processing and use of data should be brought in compliance with the new law as and when the data are used for new purposes from the time of entry into force of the new law.

If you would like to discuss any of these issues further or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com or Markus Heyder, mheyder@hunton.com.