Internet governance in September 2016:
Regional perspectives from Brazil

1. VII Seminar about Privacy and Protection of Personal Data (by Renato Leite Monteiro[1])

For the seventh year in a row, the Brazilian Internet Steering Committee (CGI.br) has held the Seminar about Privacy and Protection of Personal Data. Counting with only a few participants in its first editions, the event quickly reached it's highest attendance rate this year – showing how themes connected to privacy and protection of personal data are now occupying a central space in national and international stages.

This year's edition addressed themes regarding responsibility for automated decisions made by algorithms; big data and its impact in privacy; sharing economy; credit market and data mining; and, as it should be, the general personal data law projects.

The first panel focused in the question of the use of algorithms regarding the processing of personal data and how those, through automated decisions, may give rise to eventual practices that are discriminatory or in violation of fundamental rights. Areas such as credit concession, job offers, criminal investigations and health insurance would be among the most susceptible to such dubious analysis. Therefore, it was argued in the sense that a greater transparency would be necessary in the logic behind the personal data processing, especially in a time of massive collect and use of data through the methods that together were known as Big Data. However, the clash between the transparency level and the limits of the right to intellectual property is still a major obstacle to overcome.

Another panel addressed the Internet Bill of Rights (Decreto Regulamentador do Marco Civil da Internet) and its regulatory impact regarding personal data protection. The researchers who composed the debate addressed a few of the bill's central themes related to the use and processing of data, among them: encryption; personal data concept; electronic records; security information's requirements and patterns; and the competency to supervise such practices. One of the panel's conclusions was that the decree recommends that Internet services providers should implement the use of

[1] Digital Law Professor at the Law School at the Mackenzie Presbyterian University. Coordinator of the Law, Technology and Innovation Studies Group in this same institution.

encryption to ensure the security and inviolability of their users' communications. Therefore, unlikely what it has been alleged in some judicial decisions all over Brazil, such as those that led to the suspension of Whatsapp throughout the country, the companies that make use of encryption would be in accordance with the law, and not violating it.

One of the last panels addressed the theme of data use for credit purposes, a scene dominated by *data brokers* and algorithms known for assigning points to consumers through default risk scales, the so-called *scoring* methodologies. Representatives of private companies' who make use of those methods have exposed the importance of the data use to maintain market's healthiness, mostly in credit expansion and over-indebtedness times. However, it is clear that the existence of erroneous data about a citizen can lead to inherent harm, and that the existing prevention tools, beyond reparations, are still insufficient. As a solution, it was defended: (i) the need of an *ex ante* control, past, by the data owner part, through his consent or the use of legitimate interests, since applied adequate proportionality tests, and that the data use is done for specified and legitimate purposes; (ii) adequate governance systems, that allow the data correction; (iii) greater transparency in algorithms; (iv) and a limitation of which data may be analyzed, such as sensible data. Such points would be only a few reasons why a Personal Data Protection Bill would be necessary.

In conclusion, it was addressed the theme of the right to be forgotten, in which the most emblematic cases were quickly listed and analyzed trough the European and Brazilian conjunctures. The discussion's main point was if the decision for the content removal, based on the right to be forgotten – or the de-indexation right – may be attributed to a private entity, or if the jurisdiction should fall on the judiciary power.

All points lead to a single conclusion: even though the great majority of the general principles of personal data protection already exist in the Brazilian legal order, either expressively positivized, or by means of a integrative interpretation, there is still a lot of legal insecurity that justify the need of a Personal Data Protection Bill that would have a transversal application in all the sectors of economy and society. This conclusion reinforces the importance that this issue has garnered in the last years of discussion. And it is only beginning!

2. The new whatsApp Privacy Policy: questions to be debated under consent in personal data protection (by Bruno Ricardo Bioni)

Recently, I received an "unusual" chain message. This time, the mass text message didn't seek my evangelization about some kind of biblical teaching, even less it imprecate some kind of curse if I didn't resend it to a certain number of people.

The message had other type of indoctrination: my personal data protection. It caught my attention on how to make some kind of control over my information, because of the new WhatsApp privacy policy:

"Guys, the latest WhatsApp's update came with some thing about automatic data sharing with Facebook. Now they share your data, know who do you talk to, how often and can even use it to commercial matters. I suggest you all to withdraw this option. All you have to do is click in settings => account => uncheck the data sharing option. Do it fast, you only have 30 days to do it!"

This proactivity from the users themselves puts into doubt if they have genuinely consented to share their personal data. Or, at least, if the way they were urged to do was effective.

The message app opted for a simple signaling that it was updating its terms of service, which was followed by an alert that their consumers should accept it or stop using the app.

In this first contact, the user moment was not informed that their personal data would be exchanged with other enterprises from Facebook's economic group (the Facebook enterprise family). Only if he/she didn't immediately accept the new terms of service, by clicking on the link "read more about the updates on the terms of use/ know more", so it would be revealed the option to stop the sharing to "improve your experiences with advertising and Facebook products".

At least three questions regarding consent in personal data protection emerge in this case, in which coincide with the adjectives to it attributed by Marco Civil da Internet/ Internet Bill of rights (article 7, item IX of Law n. 12965/2014).

Informed and expressed consent

The way the terms were presented is questionable. The company may not have communicated its' users about their option to have some sort of control as to the sharing of their data in an efficient way.

From the beginning, a negative message is transmitted: in case the user refuses to promptly accept the new privacy policy, he/she cannot use the application (loses access). This emphasis tends to make a certain type of pressure under the platform users, since they see themselves intimidated by the possibility of being excluded from it. This discourages them to know more about the new terms of service and, ultimately, be aware of the option to stop the sharing of their data.

Other important fact is that the information regarding the ”automatic” cross-sharing is not revealed instantly. The user need to click on the “read more about the updates in the terms of service” option to “unbury” it. The secondary plan to which this option was delegated, reveals little transparency about what is really at stake with the changes on the terms of service. Bearing in mind that sharing option is pre-marked, it therefore becomes questionable if there is space for affirmative action on behalf of the user (data holder).

What if, instead of highlighting the service loss, they focused on the not data sharing from the start? In other words, if the first message promptly alerted the benefit using the app without the need to adhere to data sharing. And, lastly, if there was a dialogue box unmarked which would make the users to sign it in order to the users to proactively authorize that practice?

In which ways the different dynamics limit, or, on the contrary, expand the users’ cognitive capacity under the flow of their personal information? What is their impact to the purpose of qualifying the consent as being informed and express?

It’s good to remember that it is not from today that the behavioral economy alerts us about these treacherous idiosyncrasy: the cross relations mentioned above between the immediate loss of a service and the immediate gain in keeping the control over data protection can be shaken, and even manipulated.

Free consent

A much simpler question, but not least important, regards the fact that the user didn’t have the option of not sharing his or her data. The so-called ‘opt-out’ was only in terms of behavioral publicity. The “Facebook family” reserve themselves the right to process the data to other purposes – improving infrastructure and delivery systems, to understand how our services and theirs are used, improve security rules, fight spam, abuse and violation-associated activities.

Does this question the voluntariness of the acceptance of terms of service, making the object of consent vulnerable?

Next steps for these open-ended questions

It was not in vain that the Marco Civil da Internet/MCI demanded the express, free and informed consent of the data holder to third party sharing. This deep-rotted prescription seeks to promote market-associated practices capable of empowering citizens through the establishment of their own control over their data as a goal. So that there is greater transparency as to the use of their personal information, also understanding what is aligned with the national policy to the consumers relations as designed by the Code of Consumer Defense Protection (CDC) (article 4º, caput).

This is a possible dialogue - between MCI and CDC - to address the provocations on this small assay. The proposed investigation seeks to fight mystification and, in a certain way, the manipulation of the citizens self-determination power over their own data. Conversely, they will be even more dependent of chains that evangelize and imprecate curses about this topic.