Data protection, hackers and ADR. What do these things have in common?

Kluwer Mediation Blog
November 8, 2020

Andrea Maia (Mediar360 – Dispute Resolution) and Gustavo Caneiro (FGV Mediacao)

Please refer to this post as: Andrea Maia and Gustavo Caneiro, 'Data protection, hackers and ADR. What do these things have in common?', Kluwer Mediation Blog, November 8 2020, http://mediationblog.kluwerarbitration.com/2020/11/08/data-protection-hackers-and-adr-what-do-these-things-have-in-common/

Just recently (November 4th), hackers attacked Brazil's Superior Court of Justice (Superior Tribunal de Justiça – STJ). Not only they had access to the Court's system and encrypted its entire database but also demanded ransom money to restore it. In other words, they succeeded in hacking one of the most centralized courts in the Brazilian judicial system, considering it is the highest court in the country, as far as federal law suits and related issues are concerned and the last jurisdictional level before the Supreme Court, which rules on constitutional matters. From now on, STJ faces an unprecedented challenge that will be more and more common in our (not so) new data society.

We know that the STJ challenge is very unique, especially because it is a public institution, with different legal liability compared to that of private institutions. But Brazil has already had a fair amount of famous cyber security cases. Allegedly there has been a leak in the internet and telephone company known as NET of 28 million consumers' personal data (complete name, birth date, gender, IRF* number – the Brazilian equivalent to the social security number, email, telephone and complete address). Moreover, hackers posted on an internet forum that the company's stolen database was available for those interested in buying it. Later on, the company publicly announced that that data was not from their database.

In 2019, Netshoes, an online retail store, paid Brazilian Reais $ 500.000,00 (USD $ 100,000.00 aprox) to compensate for personal data leakage. The incident took place in 2017 and 2018 when personal data of almost 2 million consumers wasn't dully protected (data such as complete name, e-mail, IRF*number, birth date and clients shopping lists).

Companies should bare in mind that their database is not only another asset for their activities, but that it also involves a significant amount of responsibility and a potencial judicial liability. The Brazilian Personal Data Protection Act (Lei Geral de Proteção de Dados – LGPD) has an entire chapter (from articles 46 to 51) related to cyber security. Besides establishing several minimal thresholds for data security and also the role of the National Data Authority in these cases, the LGPD states that companies must enact governance initiatives which must count with "incident response and remediation plans" (art. 50, I, g).

Just like oil and mining companies have crisis management plans in place prior to potential crises, companies that deal with significant amounts of data, must have crisis management plans prior to the potential problem. One of the most important attitudes a company must have, is to give clear information and provide a channel for those affected by the data leakage to get any assistance needed. Check the case of Prudential do Brasil, an insurance company, that made a very user friendly public statement .

We believe that Alternative Dispute Resolution should play a central role in any of those plans, for the reasons we all know quite well. ADR will provide companies with more ways of addressing conflicts in the fast changing environment of any data leakage. Good ADR professionals must have the skills to work together with the technical cyber security professionals and authorities and translate all those interests into accessible information for those affected. Besides, it will be taken into consideration if any dispute goes to court afterwards. A good incident response plan is crucial to any company in the 21st century.