

Brazil, Canada Lead Surge In Global Privacy Law Expansion

By **Allison Grande**

Law360 (September 17, 2020, 3:43 PM EDT) -- A new Brazilian data protection law and proposed changes to Canada's privacy regime highlight the enhanced liability risks that businesses face around the world as countries race to craft personalized ways to regulate the use and sharing of personal data.

While the EU's General Data Protection Regulation and California's landmark consumer privacy law have dominated headlines in recent years, countries around the world are increasingly taking their own steps to ensure citizens' data is protected from misuse, even as legislative bodies adjust their priorities amid the global COVID-19 pandemic.

"Contrary to the slowdown in other areas, the pace of change in the privacy arena has accelerated at breakneck speed," said Lisa Sotto, head of the global privacy and cybersecurity practice at Hunton Andrews Kurth LLP. From Brazil and Canada to China and India, "nations around the world are elevating the issue of data privacy and moving full-steam-ahead to regulate it."

The issue has been propelled to the forefront by both the pandemic — which has forced more services to go digital and put a spotlight on how data is being used and shared to fight the spread of the virus — and by the rise of laws like the GDPR, which strengthened the data protection regime across the EU when it went live in May 2018.

"It's been quite busy in parliaments around the world on the privacy front, and part of the reason for that is the fact that when the GDPR went into effect, a lot of countries saw that and said, 'This is a real development. Now it's our turn to think about what we're going to do here,'" said Kurt Wimmer, the U.S. chair of the data privacy and cybersecurity practice group at Covington & Burling LLP.

The advent of the GDPR has also raised the bar for countries seeking to secure a vital declaration from the EU that they have privacy protections on par with the bloc, a status that allows personal data to flow freely between the regions.

"After GDPR, the test for adequacy is different now, so even adequate countries are looking at the possibility of changing their laws to raise them to the GDPR standards, given the importance of cross-border trade and data flows," Wimmer said. "And that's just translated into a maelstrom of privacy legislation in multiple countries."

Brazil

Shortly after the GDPR hit, Brazil enacted its own General Data Protection Law, or LGPD, in August 2018. The law, which is largely modeled after the EU regulation and is Brazil's first comprehensive data protection regulation, took effect Thursday after its original implementation date of Aug. 16 was pushed back due to the pandemic.

"With what's happened with the GDPR and in California, our legislature took the step to enact a privacy law which is very much similar to the GDPR, with similar penalties and concepts of requiring consent for asking for personal data and for accessing personal data," said Isabel Costa Carvalho, managing partner of the São Paulo office at Hogan Lovells.

The Brazilian law also goes beyond the GDPR in key ways, including by requiring all companies that handle residents' personal data — and not just those that meet a certain quantity threshold — to appoint a data protection officer and comply with the law's sweeping data access and transparency requirements, attorneys noted.

"This law will require even the bakery next door to invest in putting the proper controls and procedures in place to manage all the personal data they hold and appointing a data protection officer," Carvalho said.

The law is widely viewed as a positive development for Brazil, given its potential to boost the country's digital economy and the message it sends about how seriously it's taking the increasingly vital issue. But it's also expected to be a heavy lift for companies, particularly those that haven't had to contend with such data protection regulations in the past, attorneys say.

"This is totally new for Brazilian companies. Brazil does not have any data protection culture, so previously companies were not prepared to have any kind of documents such as these or proceedings," said Thiago Luís Santos Sombra, a partner at Mattos Filho, who is based in Brazil.

For multinationals that do business in Brazil, already being compliant with frameworks like the GDPR will serve them well, attorneys say. But they will still need to make adjustments based on the intricacies of the Brazilian law, which might be tricky for companies that have been hit hard by the pandemic and were banking on lawmakers extending the compliance deadline to the end of the year, a proposal that the Brazilian Senate recently rejected.

"We are seeing a lot of difficulties with implementing the law, and a lot of companies that are talking to us are very concerned about the uncertainty we are facing, even though they are in compliance with GDPR," Sombra said. "Today, this is the hot topic of the moment."

Sombra noted that many of his clients have new budget restrictions prompted by COVID-19, complicating the task of "implementing what's necessary in the next few months" to comply with the new law, including engaging in data-mapping exercises and preparing procedures for obtaining consumers' consent.

"You have to choose some of your priorities in order to try to find a solution," he added.

While the law went live this week, Brazil's government did agree to postpone until August 2021 the provisions that allow the country's new data protection agency to impose fines of up to 2% of the

company's annual revenue in Brazil for noncompliance.

The new regulator is still being assembled and is expected to begin by issuing key guidance on murky issues such as how to legally transfer data abroad and what qualifications data protection officers must have, attorneys noted.

But even though the National Data Protection Authority won't be going after companies right away, attorneys noted that businesses can still face immediate backlash for data protection missteps from consumers and the country's public prosecutor, who has been active on such issues in the past and can use the country's consumer protection code and other existing laws to come down on businesses.

"Data has become an asset and individuals are more aware of their rights, and companies need to be mindful that heavy fines are possible and they can't simply not pay attention to the law," Carvalho said.

Canada

While Canada already has a federal privacy law and has been recognized as adequate by the EU, two provinces are making strides toward beefing up and expanding the country's data protection regime, a development that attorneys say appears to be largely inspired by the EU and California's recent moves on this front.

"Governments and regulators in Canada are looking at other privacy regimes and comparing their regimes to that, and these frameworks in Canada haven't been updated as recently," said Melissa Krasnow, a partner at VLP Law Group LLP, who added that concerns have been swirling since the GDPR was enacted about whether Canada would be able to retain its adequacy status.

The legislature of Quebec, which along with Alberta and British Columbia are the only provinces to have enacted private-sector privacy laws, is weighing Bill 64.

Introduced in June, the bill, if enacted, would strengthen the province's law by requiring companies to implement EU-style privacy rights, introduce a new private right of action, and provide the province's data protection authority with powers to fine companies up to 4% of their global revenue for the preceding fiscal year.

"One consequence of a law like this in Quebec is that it wouldn't be exactly the same as the GDPR or CCPA, so companies would have to deal with three different ways to carry out data subject rights like deleting personal information and try to make that work across all these different regimes," Krasnow said.

Ontario is also showing signs it could enact its own privacy rules for businesses in the near future, with the province's Ministry of Government and Consumer Services issuing a discussion paper last month that referred to the GDPR as a global standard, and seeking feedback on key areas that the provincial government is considering regarding a new privacy law, including instituting data subject rights such as deletion and data portability.

"If these legislative changes are made, organizations are going to be facing an environment where there's a higher regulatory burden and enhanced risk for noncompliance, and that alone is going to change the manner in which organizations are going to have to focus on their personal information practices and dedicate resources to ensure privacy practices are being implemented properly," said

Adam Kardash, a Toronto-based partner and head of the national privacy and data management practice at Osler Hoskin & Harcourt LLP.

Discussions about amending Canada's federal Personal Information and Electronic Documents Act, or PIPEDA, have also been heating up. Federal lawmakers were expected to move this year to strengthen the federal statute, which dates to 2000, but the pandemic delayed those efforts.

However, attorneys say it's likely only a matter of time before the statute is updated, perhaps as early as next year, and that having Quebec or Ontario move quickly on their proposals would only hasten that timeline.

"It's sort of inevitable that the federal law will be modernized; we just don't know how quickly that would be," said Wendy Mee, the Toronto-based co-chair of the privacy group and the national privacy officer at Blake Cassels & Graydon LLP.

She said the hope is that if the privacy landscape gets a face-lift at both the federal and provincial levels, lawmakers "at least try to at some extent harmonize the regulations so there are not vastly different regulations across Canada and the cost of implementing these regulations isn't so huge."

India

As the second-most populous country in the world, India's drive to join the ranks of countries that have privacy and data protection laws on the books is certainly one to watch.

"There was a point at which a lot of privacy folks thought the country would simply follow the GDPR, but it looks like the country is doing more customization of the EU law than would have been expected, so the patchwork quilt continues," said Wimmer, the Covington & Burling partner.

While India's proposed Personal Data Protection bill, which was unveiled in December, shares the GDPR's core, the draft legislation "puts a lot of things on the table that GDPR doesn't do."

Those include tacking on data localization rules that would require certain pieces of critical data to stay in India, attempting to regulate non-personal information that's been de-identified or anonymized, and setting the age for obtaining parental consent for data processing at 18 rather than 16, according to Wimmer.

"It seems as if countries like India looked at the GDPR and said that they understood the structure, but Europe is a highly developed economy with 25 years experience with privacy laws, so it may not be that easy to translate the GDPR to developing countries," he said.

"So if the India law goes forward, which basically takes the GDPR table of contents and injects the substance of the law with a lot of different ideas about what's needed in a developing country, maybe that turns out to be a more compelling model for a lot of countries that don't have a privacy law yet than GDPR was," Wimmer added.

While more than 120 countries around the world already have federal privacy or data protection laws in place, roughly 80 key jurisdictions, including India, Brazil and the U.S., still lack such legislation. India's proposal is being analyzed by a special parliamentary committee and other experts in the country, and lawmakers are expected to vote on the measure early next year.

"Any global company that's going to want to do business in India, including IT and outsourcing businesses doing interesting work with data that's been great for India's economy, is going to have to find some way to deal with these changes, and hopefully imposing some of these requirements on companies won't end up harming the country," Wimmer said.

--Editing by Philip Shea and Kelly Duncan.

All Content © 2003-2020, Portfolio Media, Inc.