

Toronto / Washington DC / Brussels
www.nymity.com



Cedric Laurant

Attorney and Consultant
Cedric Laurant Consulting
Brussels, Belgium

Emerging Data Protection Laws in Latin America and Doing Business in the EU

As Latin America increases its attention to data protection legislation and regulation, a number of questions arise. Why now? What is the impetus behind their actions? What will implementation entail? Where do these countries start from in their implementation journeys? What challenges will they face, especially keeping pace with the EU and at the same time satisfying the demands of other economies, including the US, Russia, China and others with no data protection regulation?

Cedric Laurant, attorney and consultant and founding partner of Cedric Laurant Consulting provides us with a summary of the privacy challenges coming ahead in Latin America.

Cedric received his legal training in Belgium and the United States, taught courses and seminars in international privacy, data protection law and comparative law as a Visiting Law Professor at the *Universidad de los Andes* in Colombia between 2007 and 2008, and has talked at various conferences and seminars in Latin America about privacy and related issues. He directed the publication of the *Privacy & Human Rights* survey (http://www.amazon.com/Privacy-Human-Rights-Report-2006/dp/8930442897/ref=sr_1_2?s=books&ie=UTF8&qid=1315296500&sr=1-2) between 2002 and 2006, increasing its scope to cover most Latin American countries.

Cedric speaks about the current challenges for data protection in Latin America during his presentation at the IAPP Privacy Academy conference on September 14-16, 2011 in Dallas, TX (https://www.privacyassociation.org/events_and_programs/iapp_privacy_academy_2011/) and at the Public Voice conference preceding the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico City next October 31st (<http://thepublicvoice.org/events/mexicocity11/>).

Nymity: Why data protection law and regulation in Latin America today? Is it the same in all economies, or does it differ country by country?

Laurant: Latin America is the next big region after Asia that will see major changes occur in its data protection regulatory landscape. Several countries have recently gotten their act together by enacting or drafting new data protection laws. Is it a coincidence or the intent to follow the “mode du jour”? None of the above: data protection has been on the agenda of most Latin American countries at least for the past 10-15 years. What we are seeing now is an increasing political will among all states in the region to catch up with their neighbours, and a growing realization that adopting strong data protection laws will help their economies by increasing their commercial transactions outside and within their borders.

Although all countries in Latin America that currently have a data protection law or are drafting one largely follow the European data protection model, with a few differences here and there, the lack of a harmonized and integrated regional legal system like in the European Union has led countries to adopt laws or draft bills that feature many differences among each other, which creates a

diverse patchwork of legal frameworks or regulatory initiatives.

In turn, a common characteristic that appears in many Latin American privacy regimes is the constitutional right of “*habeas data*”, which despite variations from country to country, enables individuals to complain before a constitutional court to protect their image, privacy, honor, informational self-determination or freedom of information by providing them with the right to access the registries that hold their personal data, the way to amend or correct obsolete data, to insure their personal information remain confidential, and to provide means to remove sensitive personal information. Lacking from that seemingly rosy perspective is the fact that *habeas data* only provides an after-the-fact remedy for individuals and through the courts: when it requires a lawyer, it stays out of reach for most plaintiffs, to show damage may be arduous, and it relies on case law and offers poor legal certainty.

Nymity: What are the emerging regulatory highlights, by economy and what is the timeline for their regulatory implementation?

Laurant: Several Latin American countries have recently enacted, or are drafting, a comprehensive legislative framework to protect individuals’ personal information. Starting with Mexico that, since last summer 2010, regulates at the federal level the processing of personal data by businesses, and is working on implementing decrees that should become enforceable early 2012.

Follows Peru with a new data protection law that was enacted last July and now must be detailed in an implementing decree. The Peruvian law establishes a data protection authority, the “National Register of Personal Data Protection” that will keep a record of private and public databases and have the power to levy fines for violations of the law.

Colombia is still waiting for the approval of its recently enacted and first comprehensive data protection law by the Constitutional Court, which according to local counsels, should come during the last trimester of this year.

The Brazilian Ministry of Justice is working on enacting a comprehensive data protection law modeled after the European Data Protection Directive and the Canadian Data Protection Law (PIPEDA). The draft bill, which has been subject to public discussion for several months, guarantees a list of citizens’ basic rights regarding their personal data: the right to access one’s data, correct inaccurate or wrong data, delete them, object to their processing, be compensated for their misuse, and not be subject to purely automated decisions.

Costa Rica is on the verge of adopting a law that is also modeled after the EU Data Protection Directive: it regulates almost all types of personal data processing activities and requires express written consent for many of them. It would also create a new data protection authority that would be competent to issue sanctions for violations of the law. After the Supreme Court of Justice found the law to be free of constitutional defects in April of this year, the bill has made its way back to the Legislative Assembly.

Uruguay is waiting this year for the approval of its data protection law as offering adequate protection pursuant to the European data protection legal framework, after the European body of the Article 29 Data Protection Working Party issued an affirmative opinion late October 2010. Mexico and Peru might wish to obtain that European “seal of approval”, but should they follow that route, they will probably have to wait for 3 or 4 years, especially as the European Union is currently focussing its efforts on reviewing its own data protection framework.

A development worth to notice is the growing number of countries in Latin America (Brazil, Uruguay and Mexico) that have added data breach notification clauses in their data protection law, similar to the ones that exist in almost all US State statutes and are burgeoning in some EU Member States.

Nymity: What challenges will those economies face?

Laurant: A major hurdle for these countries is the questionable level of independence of their data protection authorities and the effectiveness of their enforcement means: will they obtain enough means – financial, human and material – entrusted to them by their governments to fine the companies that do not comply with the rules, and will they get the true authority necessary to enforce the new rules?

Another obstacle is the pervasive lack of awareness about data protection by the vast majority of the population: it may take quite some time before companies learn about their new obligations and implement them into their data processing activities. It will also take efforts for individuals to understand their new rights and for the authority to educate stakeholders about the new law.

At a broader level, where cross-border data transfers among all countries in the region will be at stake, the lack of an integrated regional data protection framework will give headaches to companies willing to transfer data to each other while following the legal mandates.

Nymity: How long might their journey take?

Laurant: As it is the case of all the economies that have already adopted data protection or information privacy rules around the world, it will take several years for Latin American states to fully implement them in the ground and get a high enough rate of compliance. One example might illustrate the challenges ahead: it took 20 years for Colombia, after it recognized the right to privacy in its Constitution of 1991, to come up with its first comprehensive data protection bill. It will probably take as much time for its data protection framework to reach maturity and satisfy awareness, compliance and implementation levels similar to the ones in Europe and the United States. However, to use again the example of Colombia, changes are gradual and cannot only be assessed based on changes in the law, but also through case law. In this regard, the Colombian Constitutional Court's decisions have shown exceptional clarity by building since 1992 a comprehensive case law about *habeas data* that already embodies most of the data protection principles of international data protection instruments – something some of the biggest developed economies have not achieved yet.

Among the foreseeable factors that are likely to impede the path to successful implementation of data protection rules are: a higher level of corruption than in developed economies, a much weaker public sector with limited budgets for administrative and judicial bodies, a deficit in technical expertise, a poor level of trust in the justice system and consumer protection, and a lesser degree of reliability in commercial transactions.

Nymity: What are the key challenges each economy will face from Europe? What do you recommend these economies do about these challenges?

Laurant: If these economies intend at some point in time to get the adequate protection 'seal of approval' from the EU, they will have to demonstrate that the law that exists in their books is enforced in practice and effectively protects individuals. It will probably prove harder to obtain than in the case of Argentina that was the first Latin American country to get the approval but has not delivered yet on all its promises. One of the difficulties comes from how they will protect their transborder data flows after receiving personal data from EU countries. However, the EU recognition will definitely help them with increased prospects of European investments, in particular in the business process outsourcing sector and in data and call centers.

In this context, a growing conflict has already reared its head between the United States and the European Union, each of them trying to influence Latin America in adopting its own data protection model, and multiplying commercial initiatives or courting them individually with unilateral trade agreements. Most of the progress to be done in data protection in those countries will come indeed from the economic incentives to develop commercial transactions with the rest of the world and attract investment from foreign companies, especially with the regions that already impose strict rules on international data transfers to protect their consumers. But it may not come by making each of them sign unilateral trade agreements. The European Union got started thanks to the brilliant idea of European states forming a group around a purely economic objective – build a common market and a community of countries around the production of coal and steel – then promoting within their united territory the circulation of goods, services and capital. Likewise, the same idea could be a leading factor in fostering Latin American economies to make progress on increasing international data transfers and commercial transactions: through the building of economic alliances among themselves. The best for the region is most likely to build up its own data protection model, based in part on its strong *habeas data* heritage and its civil law system, then to agree over multilateral trade treaties that would highlight the protection of international data flows as a key requirement.

Nymity: What recommendations do you have for companies that do business in Latin America? What might they begin to do to anticipate the upcoming data protection changes?

Laurant: I would advise international companies doing business throughout Latin America to embrace the upcoming data protection standards coming along in the region. Even though it will turn out to be a more costly business proposition for them, it will only be in the short term. The advice is: get an edge over your domestic and international competitors by adopting the highest data protection standards available throughout the region, and right from the start. Translating these standards to fit into the Latin American regional context means:

1. be as transparent as possible towards your prospective customers in how you will use their personal information;
2. do not be seen as following the herd of domestic companies that will probably have a harder time to comply with the new rules than you will;
3. being seen as an early adopter will be good for business and the building of your reputation;
4. in some of the countries where trust between businesses and consumers is particularly low, trust your consumers even more: it will breed reciprocal trust in your products, services, brand and reputation;
5. follow all consumer protection and data protection regulations, and go even beyond strict compliance by doing better than domestic companies;
6. develop a reputation for being fully reliable for your customers.

Nymity: What recommendations do you have for companies in Latin America that want to do business outside of Latin America? What data protection measures might they consider, perhaps in addition to their emerging laws and regulations

Laurant: If your country does not have a clear and binding data protection legal framework, lobby your Parliament members to work on one; if business is mainly with European countries, encourage your government to start the process of the “adequate protection” recognition with the European Commission. In the meantime, you will have to demonstrate that you protect well enough the personal data transferred from the EU and comply with administrative procedures and contractual steps such as signing standard contractual clauses, adopting rules that apply throughout the company everywhere it does business (“binding corporate rules”) or obtaining approval for individual transactions by national data protection authorities.

Nymity: In closing, what have we not asked that would be meaningful for our readers to know?

Laurant: Certainly there will be more information shared about the current challenges for data protection in Latin America at the next IAPP Privacy Academy conference on September 14-16 in Dallas, TX (https://www.privacyassociation.org/events_and_programs/iapp_privacy_academy_2011/) and at the Public Voice conference preceding the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico City next October 31st (<http://thepublicvoice.org/events/mexicocity11/>) and at the 33rd International Conference of Data Protection and Privacy Commissioners in Mexico City beginning on November 1st, 2011.