BRAZIL PUTS THE INTERNET TO RIGHTS

PHILIPE MOURA and **RICARDO TAVARES** look at how far Brazil's new internet law goes in terms of data privacy rights

Brazil's new internet legislation, shaped in large part in reaction to the now well-publicised excesses of the US National Security Agency (NSA), has been warmly welcomed by content and application providers although less so by the country's telecoms operators.

The legislation – Marco Civil da Internet, or Internet Civil Framework Act – was signed into law in front of an international audience by President Dilma Rousseff, herself a victim of phone tapping by the NSA. The signing launched NETmundial, the global multistakeholder meeting on the future of internet governance, which took place in São Paulo on 23-24 April. After almost five years of discussions in both houses of the Brazilian Congress, the law finally passed the night before the ICANN-sponsored meeting began.

Marco Civil was applauded by multinational over-the-top (OTT) content providers, including Facebook and Google as well as web founder Tim Berners-Lee. The telcos lack of enthusiasm stemmed from new rules on how they sell internet connectivity.

> **The government worked hard to get the law approved by Congress and it had to make concessions to secure victory.**

The new law is clear in defending the principles of freedom of expression and human rights in the context of internet governance. Its first two chapters define in unambiguous terms important principles and concepts which result in rights for internet users. The law also establishes that contracts between internet service providers (ISPs) and end-users must have a clear privacy and security clause. This clause must specify how personal data records will be stored and managed. Any clauses which "offend the protection and secrecy of private communications over the internet" are banned. And importantly, legal disputes concerning services provided in Brazil must be dealt with in Brazilian courts.

The most controversial part of the law, Section I of Chapter III, refers to net neutrality. The law reads:

"The entity responsible for transmission, switching or routing must treat equally all data packets without distinction of content, origin and destination, service, terminal or application." (Our translation)

The way it is phrased led telecoms operators to believe it placed limits on the provision of plans based on differing levels of speed and capacity, but this is not the case, according to Alessandro Molon, the law rapporteur from the ruling Workers Party (PT). He explained that operators may provide a plan with speed and capacity limits in which the speed drops once the capacity limit contracted is reached. But he spelled out there must be no preference for certain services over others at any speed or capacity level. All forms of content must be treated equally.

Another important element of the law is the strict separation between providers of connectivity (telecoms companies) and providers of internet applications (OTT).

Connectivity providers can only keep users' access details while content providers keep records of what is accessed, but all records fall under the privacy and security protections of the law. This caused some controversy because telcos claimed to be discriminated against owing to their lack of access to content use information, while civil liberty advocates were upset at records being stored for six months.

Although the law generally lacks teeth, there is one enforcement tool that allows a penalty of 10% of annual gross revenues for companies guilty of privacy violations.

The government worked hard to get the law approved by Congress and it had to make concessions to secure victory. An example of this is the stipulation that a presidential decree will determine the circumstances under which traffic discrimination or degradation can occur, an issue that affects net neutrality. The President must first get input from the Internet Management Committee (Comitê Gestor da Internet, CGI) and the National Telecommunications Agency (Anatel) before issuing this decree.

Despite this, CGI and Anatel are not explicitly considered enforcement agencies for the law, nor placed in charge of internet regulation implementation. This means the judiciary will continue to play a key role in regulating the internet in Brazil.

This is ironic because Marco Civil's goal was to establish executive branch leadership over internet regulation. With President Rousseff up for reelection in October, shaping internet regulation is particularly important at the present time. As the penetration of broadband and internet-based services increases, politicians have become more interested in regulation. Until now, the judiciary (and to a lesser extent Congress) has led internet regulation in Brazil, with the Presidency lagging behind.

The Brazilian Constitution of 1988 already

guarantees the right to privacy. The Civil Code (2002) prohibited making public or utilising any form of content related to an individual unless legally authorised or deemed necessary to ensure justice and public order.

A few positive laws apply more directly to privacy. For example, an individual can request prohibition of content usage for commercial purposes where publicity could harm his or her honour or respectability. A 1984 law ensures the national policy for information technology is based on technical and legal mechanisms to ensure the protection of the secrecy of any data stored, processed or distributed. It also protects the interests, security and privacy of both individuals and legal entities, and ensures every citizen has access to, and has the right to change and correct, any personal information in public and private databases. A more recent law prohibits the hacking of any 'information device' with the purpose of obtaining, changing or destroying data without explicit consent of the owner.

Despite the existence of these pieces of legislation the protection of privacy, particularly online privacy, has been mostly based on court precedent.

Different levels of the Brazilian judiciary have issued decisions with implications for data privacy. Those decisions refer mostly to interpretations of the constitution and the civil code, as well as enforcement of selected precedents.

One of the earliest and most notable court precedents with respect to privacy refers to a 2005 decision of a labour court on whether a company violated the privacy of an employee's email as it investigated an allegation that the employee was sharing pornographic material using the company's email. The court ruled that the rights to privacy and secrecy of correspondence applied only to personal emails that use an account other than the company's. That being the case, employers were allowed to legally track the usage and content of its employees' corporate email accounts.

In 2012, the Superior Court of Justice (Superior Tribunal de Justiça, STJ) created a precedent for how quickly content that a user finds defamatory must be erased from the web. In this case, the court of the state of Rio de Janeiro found Google guilty for taking two months to comply.

Dilma Rousseff, President of Brazil, delivers her keynote address to NETmundial

The company sought federal relief, but the STJ upheld the state court's decision against Google. The federal court decided a content provider has no more than 24 hours to remove offending content after being requested to do so.

Also addressed by the courts was the inviolability of personal information as spelt out in Article 5 of the constitution. The Supreme Court (Supremo Tribunal Federal, STF), analysed cases in which data obtained from computers was claimed to be inadmissible as evidence because it was a violation of privacy as enshrined in the constitution. The STF ruled that data obtained in authorised investigations could, in fact, be admissible because that particular case involved the transfer of public money. The court reasoned the constitutional principle of disclosing public acts superseded the right of individual privacy as the right to privacy was obstructing justice.

So court precedent has been a way of addressing legislative gaps on internet regulation in Brazil, but an insufficient one. Will the Marco Civil fill out the legislative gaps or be just a set of principles issued in an electoral year? In fact, the government is now working on a new, comprehensive data privacy and security law – which seems to confirm the idea that the Marco Civil is umbrella legislation defining general principles and trends of what is to come.

Given the government's goal of increasing Brazil's IT software and services exports to $20bn in the next ten years from $2bn in 2012, designing flexible privacy legislation that supports the free flow of data across international borders – but ensures that data privacy is protected – is a must.

PHILIPE MOURA *is research director and* ***RICARDO TAVARES*** *chief executive at Techpolis, a global ICT consultancy. See techpolis.com*