angola's cyber overkill

angola has had a very busy 2011 so far, going through a major revision to bring laws in line with the new constitution adopted in February last year. a few new laws are coming to deal with new realities such as the age of the information society. in usual angolan style, laws are dealt with and sometimes even approved wholesale in “packages” of related bills. one such package related to ICTs came before parliament in May this year, containing a bill that would seek to criminalise day-to-day activities using the internet and ICT equipment. opposition to the bill spearheaded by the sindicato de jornalistas angolanos (SJA – angolan journalists’ trade union) managed to get the bill chuckled out of the package, which went through without it. but how did things get to this point?

the first thing that should be noted is the isolation that has characterised life in Angola for decades. besides the war, Angola is surrounded by Francophonic and English-speaking countries. shielded beyond this language curtain, coupled to exorbitant hotel prices, Angola manages to stay out of range of international human rights activists and workshops on all kinds of rights, best practices and capacity building.

Plugging up the holes

it is this drive to control news that brings us to the law on cyber crimes. the catalyst was no doubt the Arab Spring. There is a difference though. Corrupt as it may be, the ruling People’s Movement for the Liberation of Angola has won every legislative election so far. the splintered opposition is weak and poorly resourced and Unita struggles to shake off its war past. so, what does the MPLA desperately want to hide? The short answer is corruption. All other societal ailments of this oil-rich country can be blamed on corruption. Embezzlement, shady privatisations, forced removals instigated by powerful people, land grabs. That is the kind of stuff that ignites society and that is what the law on internet crimes seeks to prevent.

it is about plugging up the holes in the mesh. when the papers were the problem, they were invariably dealt with either by invoking the famous criminal defamation provisions or laying charges of spreading false news, which is a crime, made easy by government sources invariably refusing to give out information. in many cases, national security could also be invoked, leaving the courts to do the dirty work. That was easy to do when the outlets were few – now the outlets are literally hundreds of thousands.

prominent embassies are those of countries with vested interests in the oil business.

journalism in a legal wild west

after years in limbo, the press law was finally approved in 2006. as the mother of all media laws, it makes provision for subsidiary laws that cater for specific media sectors and activities. Legislation on radio, television, etc, are in different stages of completion, most held in abeyance.

Public participation in the legislative process is not conducive to debate across a wide spectrum of society. Consultations involve “recognised stakeholders”, such as the SJA on media legislation. it is virtually impossible to obtain a digital copy of a draft bill. Photocopies or printed copies are handed out, making it unwieldy to distribute widely to get them under the spotlight of international rights activists.

With no law in place, a private free-to-air television station, TV/Zimbo, and a private radio station have been licensed – on an “experimental” basis, without the prescribed tender processes. The radio station, Rádio Mais, enjoys nationwide coverage, while the Catholic Rádio Eclosia, is restricted to Luanda area and Rádio Despertar (formerly the Unita radio station) was taken off the air in 2007 for broadcasting beyond its radius. At the same time, would-be applicants for community radio licences are told that they will have to wait until the law is published.

Change in tactics – replace the independent media

With broadcasting taken care of, there was only one sector left to deal with – the pesky independent private weeklies. Well-resourced media groups introduced a swathe of new newspapers, offering better quality papers and good salaries to lure the best journalists from the independent papers. in terms of the Press law, owners of media enterprises must be on record and cannot hide behind an anonymous “group”. this is not happening with Score Media, Media Investments and Media Nova – it is still a mystery as to who exactly owns these groups. All that is known is that they belong to the inner circle. this orchestrated move failed to completely take the wind out of the sails (and sales) of the independents, calling for an outright hostile takeover. Media Investments in one fell swoop bought out Semanário Angolense, A Capital and 40% of Jornal Novo – known for reporting on corruption. Concentration of media is equally in violation of the Press law.

The drive to control news is such that whereas in other sectors, including telecommunications, the foreign ownership threshold is 50%, this is pegged at 30% for media.

plugging up the holes

It is this drive to control news that brings us to the law on cyber crimes. the catalyst was no doubt the Arab Spring. There is a difference though. Corrupt as it may be, the ruling People’s Movement for the Liberation of Angola has won every legislative election so far. the splintered opposition is weak and poorly resourced and Unita struggles to shake off its war past.

So, what does the MPLA desperately want to hide? The short answer is corruption. All other societal ailments of this oil-rich country can be blamed on corruption. Embezzlement, shady privatisations, forced removals instigated by powerful people, land grabs. That is the kind of stuff that ignites society and that is what the law on internet crimes seeks to prevent.

it is about plugging up the holes in the mesh. when the papers were the problem, they were invariably dealt with either by invoking the famous criminal defamation provisions or laying charges of spreading false news, which is a crime, made easy by government sources invariably refusing to give out information. in many cases, national security could also be invoked, leaving the courts to do the dirty work. That was easy to do when the outlets were few – now the outlets are literally hundreds of thousands.
The bill on internet crimes
By its full name, the Law on Combating Crime in the Domain of Information and Communication Technologies and on Information Society Services, is part of a package of laws on ICTs, together with the Law on Electronic Communications and Information Society Services and the Law on the Protection of Personal Data.

The bill highlights the lofty ideals it aims to protect and makes the right noises about protection of copyright and combating child pornography.

But beneath the veneer, the real intent of the law is quite apparent. In their eagerness, the drafters elevated it above the Penal Code, stating in Article 6 that provisions in the Penal Code also apply to ICT crimes, “provided they don’t contradict” the provisions of this bill. Article 79 says that all legislation contradictory to the provisions of the bill is henceforth repealed. Interesting, as quite a few provisions are in conflict with the Constitution, as pointed out during the debate to block the bill.

The bill targets primarily legal persons, which makes sense as most people do not have internet at home. State institutions are exempt from the law and to add injury to insult, criminal investigators of the police and the judiciary (Angola has an inquisitorial legal system) enjoy carte blanche to search and confiscate data and in some cases even delete it without due oversight.

Penalties range from a few days to years, with most often eight or 12 years – three times that in the case of terrorist organisations. Fines are calculated on the basis of potential monthly earnings. Someone earning R15 000 a month, sentenced to eight years, would have to pay a fine of R1.45 million. A legal person will be fined three times that – R4.3 million.

Besides the astronomical fines, a company can have its operations suspended or even closed down or have its assets sold to pay the fines – and the owners will still be responsible for paying salaries while out of business. Article 4(b) makes bosses responsible for the cyber crimes committed by their workers if this happens as a result of “lack of surveillance”. That in itself would be incentive enough for bosses to control the use of the internet in the workplace.

The SJA and its partners were specifically concerned with the provisions in Article 17 as the biggest threat to freedom of the media and the work of a journalist. Article 17 is indeed unfathomably draconian. It criminalises the use of any recorded material without the express permission of those on it. So, no sound bites, no photos at events, no video material. That, even if journalists collect those at an event for which they had been duly authorised and accredited. And if the journalist received such material from a source, both are liable. Quite a blow to would-be whistleblowers.

The distribution of information with the intention of harming the country’s integrity or sovereignty constitutes a crime of terrorism. These provisions are so wide that even information of the spread of a plant disease could be classified as an act of terrorism. Anyone coming into possession – via electronic means, including a mobile phone – of any classified information – can be charged with espionage. If all else fails, the material could still be subject to perusal for any possible copyright infringement.

An attempt to commit an ICT crime is as good as committing it. Everything reverts to lowest denominator, so even accessing someone else’s equipment is as good as having gained access to the data therein. Any storage device can be pounced on as containing evidence – even text printed on a network printer. One could get two to eight years in prison plus three times the prescribed fines for “disturbing the peace and quiet” of another person if you do so using ICTs.

A pyrrhic victory
Media freedom is juicy, sexy, it commands worldwide attention and brings in knights ready to join the fight a distant fight. But now there is no fight, there will be no internet crimes bill. The government has outmanoeuvred its opponents – the ICTs legislative package went ahead without the ICTs crimes bill. So now, after “addressing” pressing concerns, the provisions in the bill will be integrated in the new Penal Code being drafted as we speak. Cyber crimes will not have a name to call it by, and any debate on the provisions will be swallowed up and drowned out in the general consultations on the lengthy Penal Code.

Hansjoerg Richter