How national interests make the EU clash with media freedoms

Ferry Biedermann- Amsterdam

The EU is about to make the use of spyware on journalists legal across the bloc. Some members states currently still have no provisions for the use of such software on journalists. But the new, ironically named, European Media Freedom Act, would allow programmes like Pegasus and Predator to be installed on journalists' devices in the interest of issues such as national security, albeit under certain circumstances. It is an example of the danger of a race to the bottom that is ever present in the bloc and that can undermine support for it on the progressive, non-nationalist, non-Brexit side of the political spectre.

The provision in the otherwise well-intentioned new legislation has caused an outcry among journalists as well as press freedom and privacy activists across Europe. Last week 80 organisations sent a letter to the European parliament urging it to ban the use of spyware against journalists altogether, saying it "puts journalistic work, freedom of expression and ultimately, democratic values in danger."

The new media act was originally devised to protect journalists and media plurality in parts of the EU where these are under pressure, as in Poland and Hungary. It claims, among others, to improve the protection of journalists' sources. But some members states, including France, reportedly, successfully pushed for extending an originally restricted carve-out that would allow spyware to be used against journalists if it was in the public interest. That was later toned down again by the European parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee that added supposed safeguards.

While in theory the safeguards should protect journalists' and the media's professional activities, in practice this is often not the case, says the European Digital Rights association (EDRi). "The European Parliament is proposing safeguards against spyware abuses that work in theory. Sadly the practice tells us something different. In France, the intelligence oversight committee had a hard time preventing unlawful surveillance of activists and trade unionists, while Romanian judicial authorities largely trust their intelligence bodies when granting authorisation to surveillance operations. The only solution is a unequivocal ban."

The new rules would create a chilling effect on journalists' abilities to pursue certain investigations, which might be what countries such as France are after. Paris has already made clear its disdain for journalistic integrity with the recent arrest of Ariane Lavrilleux, who used leaked documents to reveal a huge French intelligence blunder in Egypt that could have come straight out of the comic spy thriller OSS 117. The point being that journalists need to be able to pursue such stories in order to help rein in arrogant overreach by self-important national agencies that seek to cover their exposed backsides at all costs.

It's quite ironic that the land of liberté etc. in seeking to spare its security services some blushes allies itself with pseudo-sun kings such as Viktor Orbán and Andrzej Duda. Because spying on journalists is almost always about protecting some special interests, not about the really broad-ranging public and national interest. As pointed out in the organisations' statement above, journalism is part of the defence of democracy, which trumps any short-term, narrowly defined and ultimately misguided excuse for spying on the media.

Often, using such spyware comes down to security services making journalists do their work for them, whether it is to get close to potential targets or to close leaks. When I worked in the Middle

East, finding, meeting and interviewing terrorists was part of the job. Whatever I learned from them would then appear in print. What reason could an intelligence service have had to bug me, except in order to either find out more about such things as the movements, location, networks etc. of certain targets or possibly even to use my devices to infect those of the people I had to be in touch with? Either way of instrumentalising journalists puts them at risk or makes it impossible for them to carry out their work, if, for example, their contacts become too wary of them to even meet.

On the whistle-blower and sources side of things, the situation is even more absurd. The EU itself uses web portals to encourage whistle-blowing, for example for its OLAF anti-fraud agency. Imagine someone installing spyware on that site and weaponizing it. Claims that documents leaked to journalists put, for example, members of the security services at risk, are almost always overblown. All bona fide journalistic organisations thoroughly redact such information before making it public. Many damaging data leaks occur either through a targeted cyber-attack or by accident, when officials leave files on a train or in their car, or publish them by mistake, as happened recently with the Police Service of Northern Ireland.

Almost invariably the case for spying on journalists rests on protecting powerful structures, from embarrassment, shield them from legitimate scrutiny or on some vague notion of deterrence. While national interests are often quoted, these could also well be economic, political and so on. It is often very hard to make the distinction.

Judicial oversight of using spyware on journalists, as the European parliament's LIBE committee recommends, is of course useless in countries where the judiciary itself has already been co-opted by an increasingly authoritarian state. But even in many other countries, courts have been known to give security services a lot of leeway, as EDRi has pointed out. Cases where spyware has been used on journalists have been reported from Greece and Spain, for example.

In September Russian dissident journalist Galina Timchenko was hacked with Pegasus in Berlin. Suspicions still centre on Russia but that country is not officially a Pegasus customer. Germany is a client, as is Latvia, where her phone number is listed. And several European security agencies, including those of the Netherlands and Estonia, are known to use Pegasus outside their own jurisdiction in Europe. Whoever it was and whatever the reason, it's telling that European security agencies are not above suspicion in a case of spying on, what can be assumed to be, a friendly journalist.

It almost beggars belief to have a wholesale EU law that will allow spyware to be used on journalists. The old situation in which there was no mention of it in EU law, was preferable. At first sight it points at the dangers of EU overreach, and the question remains whether security in any case is a matter of national rather than Europe-wide rules. The spyware clause was a mistake from the start, probably an anticipated compromise, but was then extended by national governments. The problem here is not mainly one of faceless Eurocrats coming up with ridiculous or petty rules, but of powerful countries instrumentalising the EU for their own questionable purposes. Still, it is incredibly damaging, both to journalism and to the standing of the EU.