

Organised by the European Association for the Defence of Human Rights (AEDH), the European Civic Forum (FCE) and the EESC Section TEN (Transport, Energy, Infrastructure and the Information Society)

The workshop consisted of a unique panel gathering 7 representatives of the EU institutions, the civil society organisations and the digital sector. In the introduction, Mr Coulon, President of the EESC Section TEN, opened the workshop and reminded participants about EESC work in the field of cybersecurity and data protection and in particular its publication on the [ethics of Big Data](https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/ethics-big-data) as well as its opinions on the [Cybersecurity Act](https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cybersecurity-act) and the [Protection of Personal Data](https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/protection-personal-data). His introduction was followed up by a short extract of [*Nothing to Hide*](https://www.youtube.com/watch?v=djbwzEIv7gE). The 2017 open-source documentary, directed by Marc Meillassoux and Mihaela Gladovic, deals with the issue of mass surveillance. The extract broadcasted during the workshop focused on the story of Jennifer Schulte, a human rights researcher allegedly surveilled by the US intelligence services following her investigations in Somalia that revealed the participation of Americans and Saudis in a sexual traffic network in Djibouti.

The panel tackled two different but intertwined issues: on the one hand fundamental rights and on the other European sovereignty.

* Fundamental Rights

**Mario Oetheimer (FRA) presented the Agency’s publications ‘**[Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union](http://fra.europa.eu/en/publication/2018/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies)**’ which combine a mapping of the legislation related to generalised surveillance of communications in the EU Member States together with a field work in 7 of them so as to assess how fundamental rights and privacy and freedom of expression were actually protected. Oetheimer insisted that it is possible to create a proper intelligence system that is fundamental rights compliant. In this respect, the 2017 report focuses in particular on one element, i.e. the oversight framework, and the importance of including civil society actors, national human right institutions and ombudspersons. A vibrant and extremely dynamic civil society is key to ensure accountability of the overall intelligence system. He also underlined the crucial role played by whistleblowers in this area and highlighted the difficulty to ensure their protection in this particular sector due to the secrecy around it.**

**Oetheimer’s presentation was followed up by a video sent by Chris Wylie (**whistleblower) as he was unable to take part in the workshop. Wylie explains that Cambridge Analytica harvested 50-60 millions of Facebook profiles in a 2-3 months period and used them as the basis of their founding algorithms. Trough the collected information, the company was able to create tailored-made content (blogs, articles, websites) to ‘whisper’ in the ear of each and every voter hence fragmenting the society. Together with the video, Wylie addressed a particular message to the workshop participants whereby he reminded that by controlling streams of information, you are influencing behaviours and interactions and as a consequence you change the perception of reality hence making it possible to change politics since people and their culture were remodelled beforehand. In his opinion no one should be trusted and constant scepticism is the best way to apprehend information.

* European sovereignty

**Laure Batut** (EESC), President of the EESC Study group TEN/646 Cybersecurity act, confirmed the extreme vulnerability of the EU to cyber attacks and the need to develop a global approach in terms of cybersecurity. Mentioning the recent hearing of Mark Zuckerberg at the European Parliament, she mentioned the rightful intervention of an MEP that confronted Zuckerberg on his repetitive excuses that are never followed by actions since the same issues keep repeating. Batut underlined in this respect the case of Cambridge Analytica and the transfer of its databases and algorithms to a new company, Emerdata, without any precision regarding the use that will be made out of them. Batut warns not only against the GAFAM but also the Chinese companies that may not be as know as the former but have great striking power. The EESC Study Group she presides calls for the creation of a research network on securement to support the European digital sovereignty and lead to the industrial phase with the development of key technologies enabling the implementation of a true level of independent security level. To counter cyber attacks and preserve our personal data, she strongly insisted on investing in digital literacy and the continuous training of all citizens, independent of their age or socio-economic status. Despite its weaknesses, the Cybersecurity act remains an important tool to protect the citizens while enabling the latter to understand what is at stake. Batut concluded by insisting on maintaining nevertheless a proper balance between security/safety and fundamental freedoms to preserve our democratic values and principles.

**Maryse Artiguelong** (AEDH) presented the GDPR that would enter into force the following day and reminded the audience that while Member States implemented the 2001 Directive on the retention of data that reduces people’s freedoms in just 6 months, they took more than 4 years and wait for Edward Snowden’s revelations to finally agree on a text reinforcing people’s rights for data protection. The GDPR provides for an extended territorial scope of implementation, a reinforcement of people’s rights, more deterrent sanctions, the evolution of the subcontractors’ accountability, new control mechanisms as well as new obligations to data controllers. Artiguelong explained that the aforementioned GDPR’s extended territorial scope of implementation bothers the GAFAM the most as it applies to any organisation or company processing European residents’ data, even if it is not established in the EU. She underlined that from now on, European residents would benefit from additional rights such as the free, specified, informed and unequivocal consent, the right to oblivion as well as data minimisation. Artiguelong emphasised that the modernised Convention 108 of the Council of Europe has been adopted on 18 May 2018 and is, at present, the sole international legally-binding instrument in terms of data protection. Unlike the GDPR, it also covers justice and police related data. As it will be opened to the signature of international organisations, she invited the EU to sign and ratify Convention 108 in order to offer a further extended protection to the European residents. Artiguelong concluded her intervention on the need to advocate for the digital sovereignty of Europe in order to fight efficiently against data violations.

**Guillaume Vassault-Houlière** (Yes We Hack) underlined that the protection of NGOs data should not be limited to personal data as they possess a broad range of data such as staff, grass-root activists, petition signers, donators, victims, witnesses, whistleblowers, etc. that are as sensitive as personal data. He mentioned the case of a French company sentenced for the espionage of Greenpeace. Vassault-Houlière insisted on the need for the European and national institutions and agencies to finally consider providing security to NGOs as they do for companies. In his view, if the latter contribute to the economy, the former contribute to the common good and the democracy and as such they should benefit from a similar level of protection. In addition, given the context and the challenges faced by NGOs, especially from a financial viewpoint, he also recommended for the EU to boost International NGO internships in cybersecurity for the profit of NGOs, the immediate reinforcement of NGOs information systems, the maintenance of a good IT security level through trainings, the promotion of IT Security Careers as well as volunteerism in cybersecurity and the use of crowdsecurity. Vassault-Houlière finally presented the Bug Bounty’s virtuous circle.

After a Q&A session, **Jan Robert Suesser** (FCE) wrapped up the workshop. He emphasised in particular that fundamental values such as human rights and data protection should always come before economic interests. He also pointed out at the lack of awareness among the citizens about what is at stake when we talk about data protection. Suesser concluded the workshop by inviting the EESC to call for public debates\_ based on studies \_ on the following two issues:

* Is the economic model supported by the data processing companies compatible with the respect of people privacy and dignity?
* Which are the actual economical, social, well-being, psychological costs of the changes involved by the digital revolution on our societies?

**Final recommendations of the workshop**

* EU should boost international NGO Internships in Cybersecurity for the profit of NGOs and promote crowdsecurity
* EU should sign Convention 108 in order to provide an enhanced protection to EU residents and support the development of its digital sovereignty
* Control and oversight of surveillance shall be enhanced and civil society should be further involved in the oversight mechanisms of surveillance services.