Event Report: Aspen Webinar on the Ethics of Data

Human Rights vs Human Protection

14 May 2020

Rapporteur: Iulian Mihalache – Public Policy Programs Coordinator, Aspen Institute Romania

About the Webinar

The webinar was organized by **Aspen Institute Romania**, under the aegis of the **Aspen Technology & Society Program**, in partnership with the **Bucharest Office of the German Marshall Fund of the United States, Aspen Digital** and **True Story Project**. The event looked at ways in which **data and technological solutions** can **foster resilience in the face of the pandemic** and can help **contain the health crisis**. For instance, data chain owners and telecommunications operators in several European countries are already **sharing data with health authorities**, helping to fight the spread of the virus by monitoring whether people are complying with limitations on movement. Discussions addressed the **ethical aspects of the available human protection solutions** and their possible implementation in Romania. Fostering a **wider discussion on the risks and opportunities of using data flows,** the webinar sought to analyze how such measures can be implemented while at the same time respecting **human rights** and **EU's privacy laws**, such as the GDPR.

The panelists below took part in the debate, which was followed by an exchange of ideas with around 90 members of the wider Aspen community:

- Cristian Bușoi – Chair, ITRE Committee, European Parliament
- Jakub Boratynski – Acting Director for Digital Society, Trust & Cybersecurity, DG CONNECT, European Commission
- Dr. Michael Street – Head of Innovation & Data Science, NATO Communications and Information Agency
- Vivian Schiller – Executive Director, Aspen Digital, Aspen Institute US
- Joakim Reiter – Group External Affairs Director, Vodafone

Moderator: Alina Inayeh, Director of the German Marshall Fund of the United States, Bucharest Office

About Aspen Technology & Society Program

The Program represents a **platform for debate** and has created a **dedicated program community** comprising multiple stakeholders from the public, private, academic and non-governmental sectors, interested in subjects covering **technological developments and their impact on society**. The topics addressed under the framework of the Program include resilience in the context of technology-related threats, AI, Automation & Technology, as well as the impact of technology on the economy and education.

Key Take-aways, Lessons Learned and Best Practices

Discussions started from the observation that the **tradeoff between security and protection on the one hand, and human rights and privacy on the other**, already a key issue in today's technology-driven world, has become an even more topical, but also heated debate during the current pandemic. The key question is how to use available technologies to contain the pandemic while respecting people's basic rights and freedoms such as the right to privacy.

While the current context has shown that our societies have limited resilience in the face of global health crises, it has also proven the **huge potential that innovation, new technologies and data-driven solutions have in addressing the pandemic**. **Technological solutions and big data can foster resilience and be a critical tool in containing the health crisis**. Data-driven innovations offer major and concrete benefits in areas such as personalized medicine or anonymized mobility data, increasing the quality of policy-making and public services.

Participants outlined the **general framework and recent policy developments** at the EU level, which are not merely significant for containing the health crisis but also aim to **turn the EU into a global driver for data-driven society**. There is a **long-term strategy** to make Europe fit for the digital age.

In February, the European Commission presented its package of strategies for data, AI and platform regulation for the future. Its Communications on ***Shaping Europe's digital future*** and ***A European strategy for data*** and the ***White Paper on Artificial Intelligence: a European approach to excellence and trust*** have set the EU's approach towards **digital transformation**, with the purpose of turning the EU into a global role model leader. The EU aims to strike a balance by improving the **competitiveness of its digital economy** while also maintaining a **citizen-centered approach**, continuing to promote EU values and ensuring its citizens' freedoms and rights.

One of the critical ways in which technology and data can be used in the fight against the pandemic is through **mobile contact tracing apps**. By tracing people who have been in contact with infected persons, these apps can make a difference in the response against the pandemic and help societies to gradually return to normal life. Better information allows leaders to take better decisions and to make these decisions faster. Mobile contact tracing apps provide a **useful tool for governments to ascertain whether they are flattening the curve of infections or not** and whether social distancing is working the way it is supposed to. Based on movement patterns, governments can also test whether the disease is spreading from a regional epicenter to other areas and determine whether more stringent measures need to be put in place. Thus, the technology is very important in shaping public health responses, as traditional contact tracing methods are less effective due to the sheer volume of contacts. Apps can successfully complement manual contact tracing, with clear benefits related to time, the volume of contacts identified, resources spent on contact tracing, or the quality of the information received by public authorities.

However, there are also **inherent risks associated to the use of technology**, not just at the level of values and freedoms, but also regarding the effectiveness of the measures. Critics argue that contact tracing apps are problematic in terms of data privacy due to accessing locations and medical data, and that citizens are being asked to trade their privacy for public health needs. Critics also argue that the goals of public health and tech companies may differ beyond the common goal to eradicate the pandemic, with the latter having an interest in gathering data on citizens and their behavior. Furthermore, app-based contact tracing will be ineffective if it is not coupled with adequate Covid-19 testing measures. Additionally, categories most at risk include the poor and the elderly, who are less likely to have smartphones and/or use such apps.

Overall, speakers agreed on the usefulness of contact tracing apps, while keeping in mind the **recommendations of privacy experts regarding these apps**, such as:

- Sunset clauses are needed, i.e. dates for the termination of data collection and storage
- Usage of the apps must be voluntary
- Security measures must be built-in
- Apps must be based on open source technology
- There must be limits on the kind of data stored
- Companies must not sell customers' data

At the **EU level**, the European Commission and member states are also facilitating **data-driven solutions to counter the current pandemic**, **while keeping in mind the essential requirements for data privacy.** Telecommunication companies were involved in the discussion on how technology can be used to fight the pandemic more efficiently while respecting EU privacy laws. GDPR is seen by telecommunication companies as a fit for purpose, robust framework which does not impede necessary measures against the pandemic.

Following the European Commission Recommendation of 8 April 2020, member states, supported by the Commission, have developed and are updating a **common EU Toolbox on a pan-European approach for the use of mobile applications** and the use of anonymized mobility data. A common approach is important because a fragmented and uncoordinated approach across Europe would endanger the effectiveness of response measures and could cause adverse effects to fundamental rights and freedoms. The **European Data Protection Supervisor (EDPS)** further adopted guidelines on the use of location data and contact tracing tools. To ensure the full protection of citizens' privacy and data in a democratic society, applications should follow security best practices and secure-by-design principles.

In line with the goal of protecting citizen's privacy, the **EU guidelines propose several essential requirements for the national apps** that are being developed:

- Public health authorities need to authorize the app's use
- Usage of the apps must be voluntary
- Apps must be privacy-preserving, using the latest privacy-enhancing solutions such as encrypted data
- There must be no location tracking: it is important to establish whether there was a contact with an infected person, not where that contact took place
- The anonymity of data must be maintained: who the individual is is irrelevant, the purpose is collecting a large amount of data about people's movement patterns
- Apps of different member states must be interoperable, because people who are travelling need to benefit from the same functionalities.

Thus, developments at the EU-level show that there was a clear recognition of the need to act together, while making sure that the **collection of potentially intrusive data needs to be done correctly**. In order for the use of mobile tracing apps to be widespread and effective, **citizens' trust in their regulators and telecommunication companies is essential**.

The role of the private sector in the fight against the pandemic was also addressed. Apart from providing mobile contact tracing apps featuring privacy-related best practices, tech and communication companies can and have contributed through measures such as:

- Maintaining connectivity, implying massive amounts of new investments due to huge data consumption increases
- Providing connectivity services and digital applications for hospitals and medical staff, including telemedicine applications
- Providing e-learning platforms
- Providing solutions for remote work on a large scale, in particular for public administrations and SMEs.

Speakers also noted that the pandemic led to a **shift in trust** towards large private sector companies. While before the pandemic, people were reluctant to share their data, including health data, such practices have now become more widespread.