CPDP 2021 Opening Panel – Who is sovereign in our digital world?

Summary by Bianca-Ioana Marcu (VUB, LSTS)

Digital sovereignty has become an important issue at the European Union (EU) level over the past two years, culminating in the recent publication of the Digital Services Act (DSA) and the Digital Markets Act (DMA). Whilst sovereignty and 'strategic autonomy' may increasingly drive EU policy with a newly found momentum, open conversations and debates still need to happen with particular attention to what digital sovereignty will mean for European companies, politics, society, and its implications on the global dimension. The CPDP 2021 Opening Panel, moderated by Jamal Shahin, focused precisely on these topics by posing a central question: *'Who is sovereign in our digital world?'*

Defining 'data sovereignty'

In his opening presentation, Dr. Paul Timmers reminds us of the implications of the word 'sovereignty', a concept that is inextricably tied to territory, authority, and recognition, and which requires both internal and external legitimacy to function. Similarly, 'strategic autonomy' refers to the capacities and capabilities to decide and act upon essential aspects of one's longer-term future. In this context, how do we deal with *digital* strategic autonomy?

Dr. Timmers suggests that digital strategic autonomy requires an important element of risk management and avoiding extremes, a task which has been entrusted to the EU General Data Protection Regulation (GDPR). Digital strategic autonomy also goes hand in hand with strategic partnership, particularly with like-minded parties, as is elaborated by the EU Foreign Direct Investment Regulation, for example. Finally, digital strategic autonomy requires attention to the global common good under which we must strive to bring important matters, such as privacy, to the global stage.

In elaborating on the notion of sovereignty, Prof. Dr. Mireille Hildebrandt highlights its close relation to jurisdiction and territoriality, concepts which emerged in the 13th and 14th centuries. Noting the internal and external dimensions of sovereignty as mutually constitutive, the interplay between the two means that if one is broken, we will also see a threat to the fulfilment of human rights. Whilst there are scholars who present 'data vault sovereignty' as a solution in which data subjects are seen as sovereign, Dr. Hildebrandt notes that this points to the wrong use of the concept of the sovereign, which is traditionally at play between nation States.

Dr. Hildebrandt notes that many of the problems which fall within the scope of data sovereignty indeed fall within well-known issue of international law - the territoriality, nationality and personality principles, the effects doctrine, and the default non-intervention principle. Consequently, proposals around 'data vault sovereignty' contribute to giving individuals an illusory sense of control over their data, as they cannot be regarded as ruling themselves. Particularly in the context of the Internet of Things (IoT) and other real time data flows, we can see some of the challenges in exercising control over data. Dr. Hildebrandt suggests that we may draw inspiration from the German legal philosopher Jellinek who spoke of 'the normativity of the factual'. This will enable us to better understand how the facticity of data infrastructures generates a normativity that may compete with legal normativity.

Digital sovereignty: its global history and regional variations

Understanding the implications of data or digital sovereignty inevitably requires an exploration of its historical origins and how the concept is understood in regional contexts. In presenting his research on the topic, Dr. Johannes Thumfart notes how 'information sovereignty' as a norm originated in China starting from 1998 in response to US surveillance. As the prime norm entrepreneur of a territorial approach to digital sovereignty, China's norm cascades throughout the world from 2013, culminating in the EU GDPR, the World Internet Conference, and triggered by the Snowden revelations.

From 2016 until 2020 we can trace the universalisation of the norm, years in which we saw private platforms as spreaders of hostile political propaganda in the context of the U.S. general election and Brexit, and both of which resulted in calls for regulation from actors across the digital ecosystem. Dr. Thumfart takes us through the process of norm internalisation, which emerged in 2020, and in which the COVID-19 crisis triggered a new stage of digital sovereignty – one that is, he argues, here to stay. We can clearly see norm internalisation through the deployment of contact tracing apps across the world, increased content moderation, and economic bordering in the deployment of 5G.

Digital sovereignty and cybersecurity

On the basis of a common understanding of the history and definitions of digital sovereignty, Florian Pennings, Cybersecurity Policy Director at Microsoft, takes us through the cybersecurity dimension of what may also be recognised as tech-nationalism or strategic autonomy. From an EU perspective, cybersecurity policy has gained increasing support from Member States in a bid to protect industry and citizens against global threats. Cybersecurity is by definition global, not national nor regional. We have a priority to protect data and critical infrastructures based on the availability of inclusive technology, but we are also experiencing a push towards strategic autonomy via building new markets and industries. How do we balance these priorities?

One solution presented by Mr. Pennings points towards further harmonization of regulations and norms, which may allow a European version of 'digital sovereignty' to emerge. There is certainly momentum for creating more clarity in exploring regulation to establish digital sovereignty, yet it is essential for discussions in this space to avoid limiting the scope to one territory or one point of view or particular interest because cyberspace is a global space. At the same time, questions of the democratic legitimacy of policy development arise: the discussion misses the active engagement of citizens and the SME community. Mr. Pennings highlights that key debates still need to happen with all parties, and many questions still require an answer: What are the objectives of digital sovereignty as pursued by EU stakeholders such as the European Commission, and are these well aligned with both national and global objectives? From an industry perspective, how will digital sovereignty be implemented in practice? Perhaps we could take inspiration from how companies do business, rather than where they originate from.

‘Sovereignty is about insulating, not isolating’

For a flavour of the concrete steps taken to implement the concept of digital sovereignty, or strategic autonomy, Mr. Olivier Bringer, Head of Unit for the Next Generation Internet Initiative at DG Connect, outlines ongoing efforts at the European Commission. At the moment, implementation is focused on the deployment and control of critical infrastructures and technologies, with the goal of supporting a functioning economy and society. In this context, the notion of resilience and the importance of cybersecurity are highlighted as key components of sovereignty. Looking toward the future, the idea is to be sure that in 10 years’ time the EU is not left behind in the deployment of key technologies such as AI, quantum, microchips or blockchain. Investment in key technologies and infrastructures (in particular connectivity) are therefore high on the agenda.

When it comes to data sovereignty, the focus is on developing the infrastructure for a European industrial data space to maximise the benefits of the data economy, actions which require the right legal framework, the development of which started with the GDPR and is complemented by new horizontal instruments on data. The overarching idea in reaching these objectives is that our rules and values apply in the digital world, so whilst we are open to the world and companies operating within and outside the EU, they nevertheless have to follow rules relating to IP, data protection, or platforms.

Mr. Bringer highlights that we cannot be sovereign in isolation – our sovereignty needs to be connected to the world to be able to continue to attract the necessary talent and investment. The internet is global, and the fact that we work on our sovereignty and on increasing the security of our critical infrastructure is also to the benefit of the world, to citizens, and to global infrastructures alike. The EU remains a supporter of the multi-stakeholder approach, particularly when it comes to engaging the SME community and citizens in key debates on this important topic.

As we look towards the multi-stakeholder approach in the context of key technologies, David Pringle, Senior Advisor at ScienceBusiness, explores how data and AI drive progress in the sphere of open science and innovation. In order to enable open science in the area of digital sovereignty, trusted legal frameworks and trusted tools are the most important factors. Trust plays an important role because it facilitates a common regulatory base and understanding among stakeholders and enables clarity in the Digital Single Market. Beyond rule-building, common and consistent rule enforcement is also necessary, so that business and academia can operate in a climate of certainty. When we look at some of the latest developments, we continue to explore how, for example, confidential computing allows the ‘data sovereign’ to keep control over processing operations.

In the conclusion to the CPDP 2021 Opening Panel, expert speakers highlight how additional forces are at play when we discuss digital sovereignty, data sovereignty, and strategic autonomy. These themes are here to stay, and will define the structure of the Digital Transition in European Union policy in the near future. However, they also raise many questions. The balance between these questions will influence the way we interpret and identify Europe’s role as the driving force of the Digital Single Market and Europe’s role in a

globalised digital economy. Within an international digital community, and particularly in light of recent developments surrounding (social media) platforms as decision-makers, we might ask what the difference is between corporate sovereignty and territorial sovereignty.
Dr. Hildebrandt notes that whilst we indeed see major platforms exercising powers with serious consequence, we have to remember that whereas governmental power that comes from extracting assets (notably taxes) and exercising authority by way of general rules, economic power comes from sharing assets (e.g. free services) which creates dependencies. In constitutional democracies, governmental power (authority) requires treating citizens with equal respect and concern, whereas economic power does not. Commercial enterprise enjoys the freedom to contract and the freedom to dispose of its property, thus enabling a different power dynamic. Dr. Timmers highlights an additional element to this dichotomy which arises when powerful platform owners try to influence policymaking and how sovereignty is actually exercised. The convergence of the two is an area where further democratic debates are necessary, and where we again might think of how to better involve citizens in key conversations.

One of the big underlying questions is whether sovereignty as a legal and political 'tool' will remain bound to territory, control and authority or emerge as a debate around different questions relating to legitimacy, democracy and other (European) values. This brief discussion summed up a number of different perspectives on the topic, which will continue to remain at the forefront of policy and academic debates for years to come.