# Governance is essential to get digital technology right - but it needs to be more conceptualized

Eko Rahmadian

This project is funded by
**the Netherlands' Ministry of Foreign Affairs**
and managed by **Nuffic Neso**.

We are witnessing a massive increase in the use of digital technologies. This enhances the volume and speed of communication, services, trade and many other activities of people, organisations, and the government. However, there are also numerous concerns about how the rapid adoption of technologies affects security, privacy, and trust. Especially when we consider the management of sensitive and confidential information relating to health, finance, communication, mobility data, and business secrets, these concerns become urgent.

As such, securing digital platforms has become critical as confidential information is stored in software systems or digital devices. To that purpose, we have to consider several elements that may affect the security aspects of such systems: this includes the relevant stakeholders and users, as well as relevant laws and regulations. These elements enable the connectivity and networking of digital technologies, the so-called ‘digitalisation’. Unfortunately, in many cases, the relevant stakeholders have not communicated well, resulting in the failure of technology to ensure security. Therefore, to guarantee the reliability and security of digital technology, strategies are needed to govern the different aspects and to address that platform security lives up to the requirements of society and regulation where it exists.

## What is governance?

There are multiple definitions of governance. One of the most widely known refers to 'self-organizing and inter-organizational networks', where these networks complement market and hierarchical systems, and serve as the authority to allocate resources, implement control and coordination. We could recognise this concept by its characteristics: interdependence, resource exchange, rules, and significant national autonomy. Autonomy and cybersecurity itself are part of the political aspects of Digital Sovereignty or Digital Strategic Autonomy. Related to this, currently, there is a discussion around the ability of the European region to source products and services based on its own needs and values. There are concerns of negative impacts caused by overreliance on other regions in the world, or powerful nations such as China and the United States. This includes the worry of citizens losing control of their data, which has severe consequences for the privacy and autonomy. At the same time, there is not only fear about the power of states. Also private corporations gain resources and power. All of these concerns trigger a reflex of protectionism. However, such protectionism will not lead to  sustainable solutions.

From the outset, one can identify at least six governance purposes: state, corporate governance, the new public management, good governance,  socio-cybernetics systems where governance is the effect of interactive social-political forms of governing among different actors, and self-organising networks. However, the meaning of governance has changed recently. Governance is considered to be broader than the activity of the government, and also includes non-state actors, the interdependence between organisations, as well as regulation by rules that the participants of the network make themselves. Furthermore, this enhanced governance concept includes the changes in the group of participants in the process of formulation, implementation, and coordination within the network. Although these concepts of governance are quite different, they have common elements: emphasising the process of governance and the limitations of government power.

## What is digital governance?

While governance is traditionally defined as a system of norms, rules, procedures, and practices, digital governance refers to the influence of information technology on rules and practices. Datafication and the increased use of information technology provides a new environment for law and regulation. In addition, new technologies that make the flow of information and social connections possible, such as the Internet, have created new opportunities for citizen participation and organisation through the creation and content distribution. This situation is also being referred to as time acceleration in cyberspace. The acceleration of activities and engagement in cyberspace has made international and national laws unable to keep up with the pace of technological development. To some extent, digital technology has possibly changed the flow of information, the structure of society, and triggered radical social, economic and cultural changes.

Compared to the physical domain, regulating the digital domain comes with novel challenges. First, there are challenges of cyber threats and other risks associated with the digitalisation and datafication of work. Network vulnerabilities stem from the risk of using storage facilities, supercomputers, permanent connectivity, as well as misuse of private or sensitive data for harmful purposes. Even though the development of a risk prevention strategy is essential, it is not enough to defend against these attacks. Therefore, it is crucial to design a governance strategy to mitigate the potential impact caused by an intrusion or system function loss and recover from it.

Second, as law becomes an increasingly important consideration in the engineering community, there are challenges in interpreting laws and regulations as the requirements of software systems. Research in this area has solved various problems, including the extraction of legal requirements, ambiguity detection and resolution, and compliance determination. In large institutions, such challenges could be handled by legal experts. However, smaller institutions might not allow this degree of specialisation and persons with little or no legal training will have responsibility for compliance.

Third, there are issues related to privacy, network, and power attributes in digital governance that affect various stakeholders. In digital governance, the norms and roles of  each stakeholder are more fluid than traditional governance, because the relationship among the stakeholders is neither vertical nor horizontal. Thus, for the implementation of traditional governance models into digital governance, (over-)regulation may not match the technical solutions, leading to unfavourable results such as lowering the benefit of applying a digital technology. It should be reduced and transformed into the distribution of governance tasks among participants, where power is based on relationships rather than interaction based on roles or identities. We should understand that all digital projects are collaborative efforts between software developers, managers, analysts, users, and other stakeholders. Thus, it is suggested that to ensure the successful delivery of the project, the project managers should involve the stakeholders in the decision-making process at various stages of the decision-making process.

Moreover, for a digital platform that involves the stakeholders from international or extraterritorial areas, the ability to understand the values, needs, norms and regulations of each stakeholder become crucial. For example, a digital platform involving stakeholders from the European Union countries should comply with the General Data Protection Regulation (GDPR), which has emerged as an important benchmark at the international level. The adoption of GDPR has triggered a process through which other countries outside the EU have adopted or revised similar rules and regulations addressing the protection of personal data. When it comes to international data transfer, as an example, there should be an adequate system for this process that is trustworthy and reliable. If such mechanisms were in place and effective, digital platforms would gain trust from the stakeholders and the users.

## Designing a conceptual framework for digital governance

Regarding those challenges on cyber threats, law interpretations and power attributes, it is crucial to raise the awareness of each of the stakeholders. Both technological (for instance: programmer, data scientist, data engineers) and non-technological (for instance: manager, accountant, business analyst, legal person) aspects need to be included when designing rules and regulations. There are two kinds of rules that each actor should consider in the decision-making process: 1) non-technological: law, contracts, enforcement, etc; 2) technological: terms of use, code, model kind, architecture viewpoint, etc.  These rules and regulations also shape how each actor would communicate and interact when using a digital platform.

In conclusion, considering the complexity that manifests in technological systems and platforms which are a digital representation of many interrelated stakeholders, we suggested to formulate a framework to govern and support the alignment of software systems with legal regulations. Such a governance framework should be able to deliver several benefits. First, to provide a complete picture of the decision-making process in various stages. Second, to navigate how the actors could interact and communicate with each other. Third, to ensure that all processes comply with important rules and regulations by identifying relevant requirements from an early stage. Finally, to support the analysis of threat and security at various stages and provide an effective solution. Thus, by implementing this, digital technology would adapt the governance principles to gain trust from the users and all the stakeholders.

## References

- 'Erkut, B. (2020). *From digital government to digital governance: Are we there yet?.* Sustainability (Switzerland). Vol. 12 (3). Pp 1--13.
- Gstrein, O. J. & Zwitter, A. J. (2021). *Extraterritorial application of the GDPR: promoting European values or power?.* Internet Policy Review, 10(3).
- Gstrein, O. J (2021). *A Call for a Value-Driven Approach to Digital Sovereignty.* Israel Public Policy Institute.
- Hill, R. (2014). *The internet, its governance and the multi-stakeholder model.* Info. Vol.16 No 2, pp.16-46
- Klijn, E. (2008). *Governance and governance networks in Europe: An Assessment of ten years of research on theme.* Public Management Review. Vol 10 (4). Pp 505--525
- Mc.Manus, J. (2004). *A stakeholder perspective within software engineering projects.* IEEE International Management Conference 2004.
- Rabinia, A., Ghanavati, S. (2017). *FOL-based approach for improving legal-GRL modeling framework: A case for requirements engineering of legal regulations of social media.* IEEE 25th International Requirements Engineering Conference Workshops, REW 2017. Pp 213--218
- Rhodes, R.A.W. (1996). *Understanding Governance: Policy Networks, Governance, Reflexivity, and Accountability.* Open University Press. Buckhingham Philadephia.
- Rhodes, R.A.W. (2007). *Understanding Governance: Ten years on. Organization Studies.* Vol 28 (8). Pp 1243--1264
- Sharp, H., Finkelstein, A., Galal, G. (1999). *Stakeholder identification in the requirements engineering process.* 10th International Workshop on Database and Expert Systems Applications. DEXA. 1999.
- Treib, O., Bähr, H., Falkner, G. (2007). *Modes of governance: Towards a conceptual clarification.* Journal of European Public Policy. Vol. 14(1). Pp 1--20
- Zwitter, A., Hazenberg, J. (2020). *Decentralized Network Governance: Blockchain Technology and the Future of Regulation.* Frontiers in Blockchain. Vol 3 (March). Pp 1--12