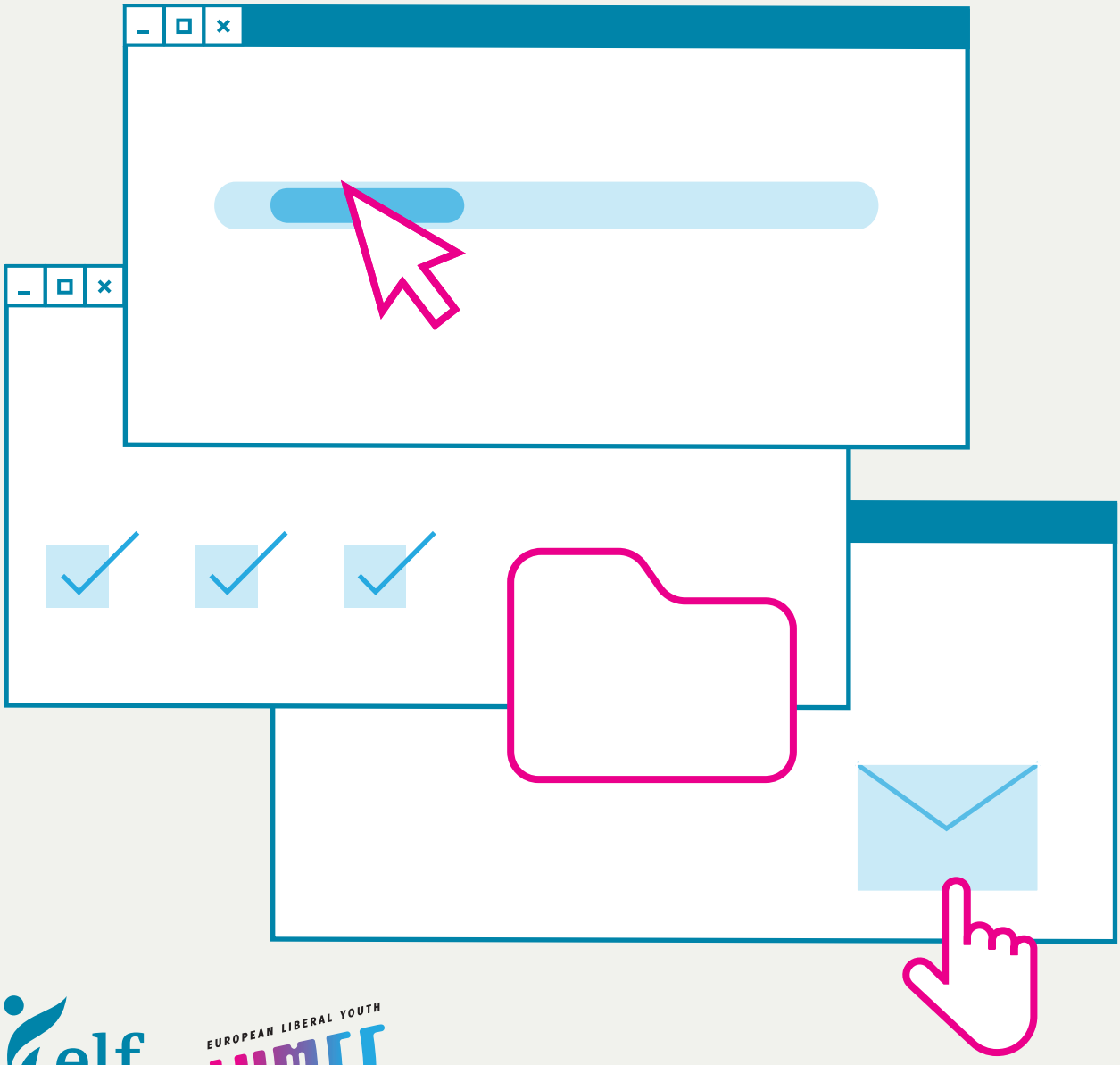
A ROADMAP ON E-GOVERNANCE FOR YOUNG LEADERS

This roadmap is a continuation of the European Liberal Forum project "Young Leaders Meeting 2020, supported by LYMEC"

By **Kevin Tammearu**



elf

EUROPEAN LIBERAL YOUTH
LYMEC

Contents

Kevin Tammearu

Kevin is an international business development executive with experience in building relationships and strategic communications. He has collaborated on launching two new initiatives and the rebuilding of a 20+ years old Chamber of Commerce from a PR perspective. He has led 9+ trade missions between the UK and Estonia. He is a former Bureau member of LYMEC - European Liberal Youth.

Introduction

Good governance and public administration are inherently challenging tasks given their multi-stakeholder nature and the ever-changing demands and needs of citizens. And perhaps it is the challenging nature that calls upon liberal-minded and entrepreneurial leaders to emerge[1], take up political, administrative and organizational leadership positions and drive meaningful, positive change through the channels of digitalization and innovation. However, some conceptual frameworks need to be considered for this change to be feasible and for it to be sustainable.

It would seem appropriate to consider that technology can bring forward this type of positive impact because there is an abundance of great examples of this from around the world[2]. However, over the past decade or so we have also witnessed how technology and platforms can have very damaging impact on society, our democracies and freedoms[3]. Technological advancement should not negatively balance our fundamental freedoms and rights.

With this in mind, the "ELF Young Leaders Meeting 2020" supported by LYMEC focused on the future of society from the perspective of digitalization and innovation in governance and public administration. The key balance to strike in this case revolves around (1) providing citizens additional and more efficient means to engage with the state so that society can focus on productive tasks rather than compliance with bureaucracy and (2) making that possible in a way that citizens' safety, freedoms and integrity are not infringed upon.

This short report acts as a primer for political and organizational leaders by offering a conceptual framework of the components enabling e-governance together with essential considerations about digital transformation of public administration. With this in mind, the report ties several topics together as part of a wider narrative: industrial revolutions; the role of government, public administration and their evolution; the future perspective of e-governance and the key enablers.

1. Fourth Industrial Revolution and the digital society

The speed at which technological progress happens is exponential[4], while deeply rooted societal change can take generations. This is to emphasize the unique impact new technologies have on society's evolution. We no longer have ample time to consider and analyze the changes we are experiencing. Among other things, this poses challenges to public administrations in overcoming legacy systems and achieving high levels of e-governance.

In "Sapiens" Yuval Noah Harari[5] eloquently explains how as *homo sapiens* we've gone through three major revolutions:

- the **cognitive revolution** with emergence of language around 70 000 years ago;
- the **agrarian revolution** with domestication of plants, animals and emergence of settlements around 12 000 years ago;
- and the **scientific revolution** 500 years ago with human kind recognizing its ignorance, the emergence of capitalism (and industrialization as a subset of this revolution).

These changes can be illustrated as periods where for a while nothing happened, then something happened, which was followed by not a lot happening again. Change in terms of industrial revolution however sees a lot happening for a while followed by a lot more happening. From the end of the 18th century we've gone through three[6] and are witnessing the 4th industrial revolution[7]. These are characterized by emergence of new technologies and change in perception of the world that trigger deep economic and social changes:

- The **First Industrial Revolution** brought forward mechanical production, the steam engine and gave way to urbanization. The backbone of societal economy started to shift from agriculture to industry.
- The **Second Industrial Revolution** came with the emergence of greater scientific advancement and mass production, electricity, methods of communication, the automobile and airplane. Industry was now the backbone of societal economy.
- The **Third Industrial Revolution**, also considered the Digital Revolution, was enabled through semiconductors, mainframe computing, personal computing, internet and high-level automation. The backbone of societal economy started to shift from industry to service and knowledge work.
- The **Fourth Industrial Revolution**[8] is something we are going through today and is characterized by the merger of technologies that blurs lines between physical, digital and biological spheres. These changes will transform systems of production, management and governance.

1. LYMEC, Press release – Young Liberal Leaders "European Liberal Youth asking for a single EU citizen number", Brussels, (October 2020)
2. United Nations, e-Government Survey, (July 2020)
3. The Atlantic, "What Facebook Did to American Democracy", (October 2017)
4. Rosner, M., Ritchie, H., "Technological Progress", (2013)
5. Yuval Noah Harari, "Sapiens: A Brief History of Humankind"
6. Encyclopedia Britannica, "Industrial Revolution", (September 2020)
7. Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond", (January 2016)
8. World Economic Forum, "What is the Fourth Industrial Revolution?", (January 2016)

Now the challenge here is that with the Fourth Industrial Revolution knocking on our doors, most governments and public administrations around the world are struggling with implementing benefits from previous ones. We use electricity, computers, internet, information systems and so on, however the challenges of using the advantages of previous revolutions in public administration to their full extent are more nuanced and still lacking even in countries with high levels of social and economic development[9].

While Europe maintains a relatively good standard of living, one billion people live without constant supply of electricity[10] also extending to public institutions and businesses in those countries. Even though there is widespread use of computers and internet, only a few countries[11] have been able to digitalize public services in a way that makes their approach sustainable and enables the emergence of a mature e-governance setup[12].

The digital revolution has brought forward a loosely defined term "digital society[13]" which looks at the full digitalization of public administration together with other spheres of life. This approach is generally in line with the belief liberals hold[14] towards the role of government, the state and public administration.

The general view here being that – while the modern state has taken on other roles beside securing life, liberty and property – governments should provide an environment in which citizens, businesses, NGOs etc. can function to their full potential and use their precious time for value-added activities. Standing in queues at public offices and agencies in this case not being a valuable activity and as such should be made as simple and efficient for the citizen as possible.

2. Role of government and public administration

We can place the challenges the lack of digitalizing the public administration can pose within a wider context of societal change. However, it is also highly relevant to consider what would be the reasonable role of government and public administration when it comes to reforming itself.

If we look at the EU level Digital Economy and Society Index[15], then we see 5 areas of overall development and maturity of countries as it relates to digitalization in general:

- **Connectivity** – fixed broadband take-up, coverage, mobile broadband and broadband prices;
- **Human capital** – Skills and advanced skills of internet users;
- **Use of internet services** – Citizen's use of internet service and online transactions;
- **Integration of digital technology** – Level of business digitisation and e-commerce;
- **Digital public services** – Level of e-government development.

If we expand on the term "digital society" discussed in the previous chapter, we can see that the EC sees it consisting of several components out of which digital public services and the level of e-government development is only one. This is relevant to keep in mind when conceptualizing what a digital society stands for and comprises of, as e-governance and the digital transformation of public administration only stands for one element of a wider societal process.

While there are other areas within the scope of e-governance such as e-democracy, e-participation, e-communities etc. then the focus here is on what can be considered the most straight-forward of them: e-services, digital services. This considers the role of the state in providing services to citizens and businesses through traditionally physical means: a person going to an agency to interact with an administrator, possibly doing that several times and to several agencies to receive a service. In this sense, an interaction which – when digitalized – provides a very tangible benefit to the population.

The role that political and organizational leaders[16] should carry in this particular case revolve around three main areas: leadership, environment and implementation[17]. Leadership in this context means that developing and projecting the overall vision of governance – and as a result e-governance – stands on the shoulders of political and organizational leaders who communicate this to the public and develop the message into more granular nuance. There are several examples[18] of political leadership being placed at the very top in terms of prerequisites[19] of sustainable e-government adoption within a country. In essence this refers to political leadership being a key element that enables countries to spearhead challenges revolving e-government implementation. This also means that the wider public administration gathers their direction and motive from the vision set forth and projected by political leaders.

9. European Commission, The Digital Economy and Society Index, (October 2020)
10. World Bank, Access to Energy is at the Heart of Development, (April 2018)
11. The Conversation, "Digital Government isn't Working in the Developing World. Here's Why." (September 2018)
12. This is explored further under the "Evolution of Digital Public Administration" paragraph of this report
13. e-Es a Briefing toni Centre, https://e-estonia.com/
14. Depending on where one stands on the spectrum of liberalism.
15. European Commission, The Digital Economy and Society Index, (October 2020)
16. Those in leadership positions in public entities such as ministries, agencies, departments etc.
17. Rabaiah, A., & Vandijck, E., (2009). A Strategic Framework of e-Government: Generic and Best Practice,
18. The New Yorker, "Estonia the Digital Republic", (December 2018)
19. Chernov, Serhii & Haiduchenko, Svitlana & Bielska, Tetiana & Naplyokov, Yuriy & Arjjumend, Hasrat. (2018). Leadership in the Context of E-governance: Lessons for Ukraine. Grassroots Journal of Natural Resources.

Providing a regulatory framework for public sector organizations to innovate and digitalize their operations also lays on the shoulders of government in general[20]. There should be legal and policy frameworks[21] in place that are in close relationship with what the current state of the art is in specific fields, but also that these frameworks actually make it simpler for agencies to re-engineer their processes, offer services in novel ways and engage the users of their services.

The OECD considers the aspect of policy frameworks in their Digital Government Index[22]. In their view a mature digital government has government policy frameworks in place that enable a public sector that is digital by design, data-driven, acts as a platform, open by default, user-driven and proactive.

Once it comes to implementation, it is relevant to keep in mind that e-governance doesn't have an ending. As long as there are people, there will be governance and one should keep in mind that implementing novel approaches in what are typically slow changing organizations is an iterative process. There will be a balance between learning from best practices and also from one's own experience and experimenting, as countries will have to adapt know-how to their local context.

The other side of the coin with implementation is that government and the public sector should resist the urge to do everything themselves. There is deep industry knowledge and practice in most areas of technology and e-government. It makes more sense to build on that expertise through collaborations and partnership with the private sector and NGOs in developing and delivering state of the art solutions for the public[23]. Public-private partnerships can have different models, whereby private entities can host and operate services on behalf of the government, for the government or develop some elements required for providing the service (such as underlying technology).

3. Evolution of digital public administration

Noting that digital public administration as an extension of governance has no end in sight, it's relevant to keep in mind that digital public administration has stages of evolution. Every country doesn't necessarily have to go through all of them, however there are logical steps of progression through simpler means towards more complex iterations.

One of the most cited models – and e-government papers – to measure maturity of e-government is the Layne and Lee[24] four-stage model, which consider technological and organizational complexity in relation with integration. The technological and organizational complexity ranges from *simple* to *complex* and integration from *sparse* to *complete* or *seamless*. The four stages of development are catalogue, transaction, vertical integration and horizontal integration. Essentially going from having

- **online presence** (a website) and downloadable forms to
- having some **forms and services online** with a database supporting it, to
- **integrating databases and systems within a domain** (like education or health) and finally
- **integrating systems across different functions** and providing citizens with a one-stop shop experience (like a citizen portal).

While this model has been highly influential, it's relevant to keep in mind that all models are products of their time, context and mindset.

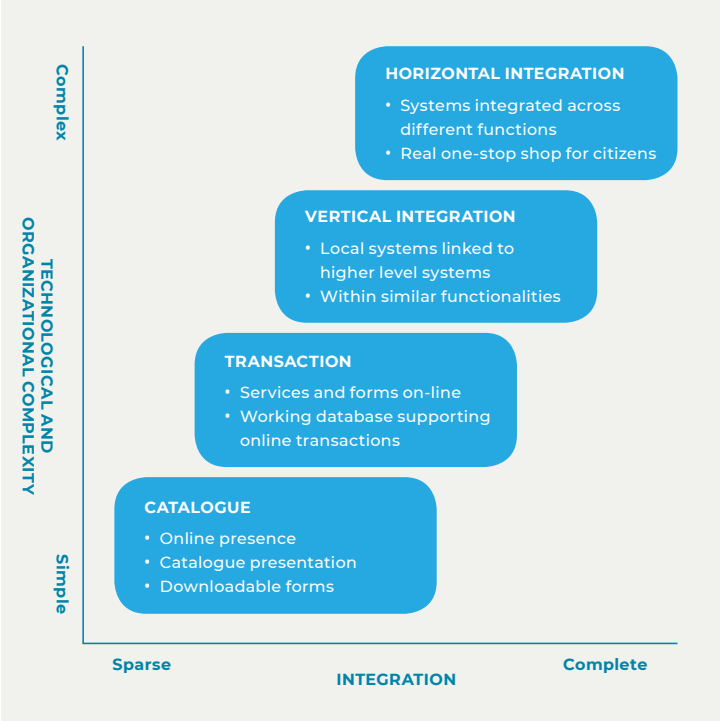


Figure 1 Layne, K. & Lee, J. (2001) Developing fully functional e-government: a four-stage model

20. There is a great deal of reluctance from governments to engage the private sector in developing, delivering and operating public services. This is in essence a wider topic of the roles modern government has taken. The empirical evidence in relation to e-governance suggests that the more successful cases are where there is close collaboration between the private and public sector. In a way this is in line with liberal thought towards governance.
21. European Commission, Policies on eGovernment
22. OECD, Digital Government Index, (2019)
23. e-Governance Academy, e-Governance Conference, "Public-Private Partnership Models in e-Government Development", (May 2020)
24. Layne, K. & Lee, J. (2001) Developing fully functional e-government: a four-stage model, *Government Information Quarterly*, 18(2), 122-136

That's why there is an abundance of different models[25] with different names of stages, number of stages, meaning of stages and also an abundance of comparative reviews of these models[26].

These models aren't necessarily meant to be taken as roadmaps for governments implementing e-governance, but rather act as a tool for making an assessment to understand where they lie in terms of development. This should fit in the context that within an administration not all agencies and organizations will enjoy similar levels of digitalization. Some might be making their very first steps in overcoming their legacy thinking and systems, while others might be born digital and have all the capabilities to engage in horizontal integration and look towards the next stages.

Today we see that even though these models exist and are published, the main challenge remains around implementation and progressing towards horizontally integrated e-governance[27] - the "fourth stage" in the Layne & Lee model with which most administrations struggle with.

4. The future perspective of e-governance

The future perspective of e-governance derived from some of these maturity models suggest that once there is horizontal integration between organizations and technology, then steps such as e-participation, e-democracy, forecasting or the provident stage[28] emerge. In these later, mature stages e-governance utilizes new technological advancements in big data and artificial intelligence together with applications and channels provided by the private sector to enable an even faster and smoother experience for citizens (ibid.).

While it will still take time for industry practice to emerge here, it might be simpler to conceptualize that e-governance development stages progress from physical interactions (going to an office) to digital interactions, from vertical integration to horizontal integration. However, it is also important to keep in mind that this development should progress from reactive to proactive services.

Assuming there is horizontal integration and a one-stop shop experience within a specific domain, it is still expected that a process is started by the citizen engaging through these digital means. Horizontal integration should however provide an experience where generic tasks are automated to the extent that they function in the background without the citizen having to initiate them.

A simple example to think of is with expiration of passports, ID-cards or drivers licenses – these services can be designed in a way that a citizen is simply notified that the respective agency has issued a new identification document for them. Or for instance when a child is born, they are automatically registered, given a unique identifier (e.g. in the case of Estonia[29]) and the parents are automatically signed up for child benefits.

5. Key enablers of e-governance:

With the notion that there are several stages in e-government maturity and a sense of the aims and aspirations a public administration should have in digitalization, it then makes sense to cover what are the key functional[30] enablers for an e-governance setup that can achieve a certain level of maturity.

In general, these key enablers revolve around the aim of making it possible to achieve the later stages of maturity models and provide services to citizens. If services are the target, then the functional starting point for this revolves around data, databases and government registries, as they are crucial in providing services.
And the enablers are what make it possible and feasible to transform data into meaningful and secure services:

- **interoperability** and **secure data exchange**;
- **Digital identity**, **secure authentication** and **digital signatures.**

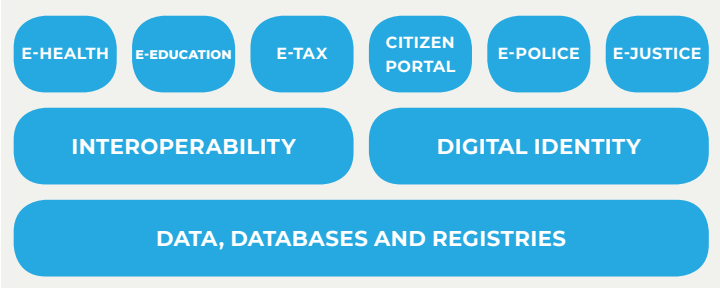


Figure 2 A conceptual architecture, key functional enablers of e-governance

25. Chaushi, A., Chaushi, B. A., & Ismaili, F. (2015). Measuring e-Government Maturity: A meta-synthesis approach, *SEEU Review*, *11*(2), 51-67
26. Fath-Allah, Abdoullah & Cheikhi, Laila & Al-Qutaish, Rafa & Idri, Ali. (2014). E-Government Maturity Models: A Comparative Study. International Journal of Software Engineering and Applications. 5. 71-91. 10.5121/ijsea.2014.5306.
27. Elnaghi, Marwan & Alshawi, Sarmad & Missi, Farouk. (2007). A Leadership Model for e-Government Transformation.
28. Draheim, Dirk & Erlenheim, Regina & Pappel, Ingrid & Janssen, Marijn & Lemke, Florian & Taveter, Kuldar. (2019). Stage Models for Moving from e-Government to Smart Government.
29. Estonian Ministry of the Interior, Population Register
30. This chapter looks at functional enablers. It should be kept in mind that there are other enablers or prerequisites such as legal environment, digital literacy and education, a school of thought in public administration etc.

In a simplified way, we need data to create and provide services. Given that services will need to combine data across a number of different, independent organizations, there has to be an interoperability framework and solution between the public organizations to integrate databases and registries. And once there are services created, we need to enable citizens to use them without restrictions in comparison with physical, analogue use – to securely authenticate themselves online and provide digital signatures with legal value – like a signature on paper.

5.1 Data, databases and government registries

Governments have been collecting and storing data and information for as long as there has been governance[31] – keeping some form of records about population, governing decisions, private property etc. etched on stone tablets, papyrus, paper.

There are several challenges when it comes to data storage and use. Providing services to citizens in a meaningful way expects that data will be shared among government (and in cases private sector or NGOs) entities and across domains. The intuitive response would be to pool data together under a single roof so that it would be easier to access it. In effect, this intuitive response creates what would be referred to as super databases. This brings an abundance of challenges such as increasing the likelihood of misuse, malicious intent, single points of failure and global bottlenecks and should not be the preferred direction.

The questions are around how to preserve integrity of the data, make it possible for organizations to access data to provide services that they've been mandated to provide but also avoid infringing on their legislative independence and creating honeypots for malicious intent[32]. And on top of that, it is also important to avoid duplication of data across different organizations – so that there wouldn't be different versions of the same thing[33].

Solving these challenges requires implementing means within policy[34] and technology. An example from policy is enforcing a once only principle[35] across the public administration. This essentially means that government should ask a specific kind of data from citizens and businesses only once.

This means that once government has this data, it should be shared among other entities utilizing interoperability and secure data exchange capabilities in a way that avoids data duplication. From a citizens' perspective government is a single entity and from a good governance perspective, whole-of-government approach should be preferred when going through digital transformation. By means of policy then, some entities are given a mandate to maintain a specific type of data, such as a persons' address or their education history. They are custodians of the data and act as a 'single source of truth' for this data – everyone else asks this data from them by querying it when it is necessary in providing some service or fulfilling some tasks. And it is imperative that these queries are based on the mandate this organization has – a legal basis for asking and processing this data.

Enforcing this principle expects that there is a policy measure in place whereby there is a single source of truth for specific kind of data. Every other organization that needs this specific data will query it from the custodian of that data. As an example, if the population registry maintains information about what is your registered address, then the tax authority in their processes would query that information from the population registry and not ask it from you or create a duplicate of that in their databases. Services should then be designed around these principles.

The technological aspect here is also around protecting the integrity and confidentiality of data. These challenges are mostly solved through the use of secure access, cryptography and enforcing those means through policy[36]. In a simplified way this means that data should be encrypted at rest and databases, registries should keep records of any changes made to data

5.2 Interoperability and secure data exchange

Once there is data that is managed by specific organizations, other entities will need a standardized framework to access that data in order to avoid the inefficiencies of developing integrations one-by-one and rather re-use available components. This is achieved through the implementation of interoperability frameworks and secure data exchange solutions.

Interoperability[37] in this context means that independent organizations should have standardized ways of exchanging data with each other. If we have independent organizations who hold a specific kind of data, to which they are the single source of truth, then there will be other organizations who need this data to provide complex services within their mandate.

31. Brosius, M. (ed.). (2003). *Ancient archives and archival traditions: Concepts of record-keeping in the ancient world*. Oxford: Oxford University Press.
32. Priisalu, J., Ottis, R. Personal control of privacy and data: Estonian experience. *Health Technol.* 7, 441–451 (2017)
33. Baheer, Baseer & Lamas, David & Sousa, Sonia. (2020). A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects. Administrative Sciences. 10. 25. 10.3390/admsci10020025.
34. Ministerial Declaration on eGovernment, the Tallinn Declaration, (October 2017)
35. European Commission, CEF Digital, Once Only Principle
36. Digital Guardian, Data Protection: Data in Transit vs. Data at Rest, (July 2019)
37. National Interoperability Framework Observatory, Interoperability

Considering the information security implications described above, we should avoid the creation of super databases, interoperability in its essence favours a distributed architecture where each organization maintains their independence and the data they hold. Interoperability creates the standardized environment in which its possible to securely exchange data so that organizations interact with each other peer-to-peer, without a central intermediary and using encryption for the exchange of data.

While there is no central component through which all the data should flow, there needs to be some form of central coordination or governance. In e-governance this typically suggests that there is an agency in charge of providing other organizations a service for secure data exchange and interoperability. The tasks of this agency include things like setting the security policy, onboarding and educating organizations, developing additional measures to improve security, scalability and user-friendliness etc.

And naturally, interoperability and secure data exchange solutions should log all of the data exchanged between organizations, so that it would be possible to use these logs as evidence in disputes. This serves the purpose of providing transparency to citizens about the use of their data, but also guarantee a secure environment to the administrators who are using this data in their daily work. This means that a public administrator querying data from another organization needs to have assurances that the data hasn't been altered in transit, but also that if they use this data to make a decision that is disputed, it is possible to later prove where the liability stands. There are various methods a malicious actor might use, such as a Man-in-the-middle (MITM) attack where the actor positions themselves in between the application and a user or in between two counterparts exchanging information and acts as if normal exchange of information is happening.

There are several measures in countering and avoiding these attacks and malicious use. This is primarily the concern of information security. The cornerstone of information security is considered to be the CIA triad: Confidentiality, Integrity and Availability, which has been broadened to consider additional information characteristics, states and security measures. A good primer on this topic is to look at reference models of information assurance and security (IAS)[38]

5.3 Digital identity, secure authentication and digital signatures

If there are services developed based on authoritative data that is usable across domains and verticals, there should also be means to access these services securely. Digital identity in this sense provides us with two means: secure authentication and digital signatures.

In a simplified way, we need to have digital equivalents of two activities we would do in the physical world:

- When going to an agency to receive a service, we need to authenticate/identify ourself using a document such as passports or ID-cards;
- Once we have proven our identity, we need to provide a signature as proof of our consent towards an action.

Secure authentication means that there have to be measures to access services, portals, information systems etc. in a secure way. The traditional username and password combinations typically do not suffice for the level of assurance government transactions need and some of the most successful implementations[39] of this have been through the use of public key infrastructure or PKI[40]. Digital identity should use a whole-of-government approach and use across different domains and organizations. This gives us a federated identity[41] – every service provided by the government can be accessed using the same means of authentication.

Examples of this can also be seen from the private sector – large industry leaders such as Facebook or Google provide federated authentication, where third parties or smaller companies use these existing identities to provide access to their services. Think about the applications where we use our Facebook or Google credentials to log in. In a way government provided digital identity is similar, however the security considerations in providing them are vastly different.

The digital signatures side of digital identities revolves around consent and proof of desire. In the physical world the equivalent for this is a handwritten signature. Digital signatures make it possible to provide this using – again – complex mathematics and cryptography, but also legislative means so that there is legal basis in giving and accepting digital signatures[42]. Benefits of digital signatures surpass the use-case of government services and can also be utilized in signing transactions (banking) or legal documents such as agreements, contracts etc.

38. CHERDANTSEVA, YULIA & Hilton, Jeremy. (2013). A Reference Model of Information Assurance & Security. Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013. 546-555. 10.1109/ARES.2013.72.
39. e-Estonia Briefing Centre, e-Identity & ID-Card
40. Public key infrastructure, https://en.wikipedia.org/wiki/Public_key_infrastructure
41. Derrick Rountree, Chapter 2, "What Is Federated Identity?" Federated Identity Primer, (2013)
42. European Commission, Trust Services and Electronic Identification

Conclusions

Liberal political leaders are at the core of making e-governance reforms and digital transformation of public administration a reality that works for everyone. Given the remarkable speed at which technological change is happening and the way it is pressuring changes in societal behaviour, it is critical that governments achieve high levels of e-governance maturity.

The current low hanging fruit is to achieve levels of maturity that encompass horizontal integration, as that paves the way for more complex forms of e-governance. This includes implementations of e-democracy, e-participation and foresight that would not only respond to the needs of 21st century citizens, but also support our societies in managing complex changes.

The key elements that support this effort revolve around putting in place functional pieces within the e-governance concept. This starts with data, databases and registries and moves towards providing citizens services that respect their time. Ideally these services are proactive in a way that requires the least amount of effort from the citizen. In between lay digital identity and interoperability as the key enablers of a mature and secure digital government and digital society.

It is efforts such as the "ELF Young Leaders Meeting 2020" supported by LYMEC and others of its kind that drive this type of meaningful change and political dialogue which sets the focus on the future of society from the perspective of digitalization and innovation in governance and public administration. The key balance to strike in this case revolves around (1) providing citizens additional and more efficient means to engage with the state so that society can focus on productive tasks rather than compliance with bureaucracy and (2) making that possible in a way that citizens' safety, freedoms and integrity are not infringed upon.

Bibliography

Baheer, Baseer & Lamas, David & Sousa, Sonia. (2020). A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects. Administrative Sciences. 10. 25. 10.3390/admsci10020025.

Brosius, M. (ed.). (2003). *Ancient archives and archival traditions: Concepts of record-keeping in the ancient world*. Oxford: Oxford University Press.

Chaushi, A., Chaushi, B. A., & Ismaili, F. (2015). Measuring e-Government Maturity: A meta-synthesis approach, *SEEU Review*, *11*(2), 51-67

CHERDANTSEVA, YULIA & Hilton, Jeremy. (2013). A Reference Model of Information Assurance & Security. Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013. 546-555. 10.1109/ARES.2013.72.

Chernov, Serhii & Haiduchenko, Svitlana & Bielska, Tetiana & Naplyokov, Yuriy & Arjjumend, Hasrat. (2018). Leadership in the Context of E-governance: Lessons for Ukraine. Grassroots Journal of Natural Resources.

Derrick Rountree, Chapter 2, "What Is Federated Identity?" Federated Identity Primer, (2013)

Digital Guardian, Data Protection: Data in Transit vs. Data at Rest, (July 2019)

Draheim, Dirk & Erlenheim, Regina & Pappel, Ingrid & Janssen, Marijn & Lemke, Florian & Taveter, Kuldar. (2019). Stage Models for Moving from e-Government to Smart Government.

e-Es a Briefing toni Centre, https://e-estonia.com/

e-Estonia Briefing Centre, e-Identity & ID-Card

e-Governance Academy, e-Governance Conference, "Public-Private Partnership Models in e-Government Development", (May 2020)

Elnaghi, Marwan & Alshawi, Sarmad & Missi, Farouk. (2007). A Leadership Model for e-Government Transformation.

Encyclopedia Britannica, "Industrial Revolution", (September 2020)

European Commission, CEF Digital, Once Only Principle

European Commission, The Digital Economy and Society Index, (October 2020)

European Commission, The Digital Economy and Society Index, (October 2020)

European Commission, Trust Services and Electronic Identification

Fath-Allah, Abdoullah & Cheikhi, Laila & Al-Qutaish, Rafa & Idri, Ali. (2014). E-Government Maturity Models: A Comparative Study. International Journal of Software Engineering and Applications. 5. 71-91. 10.5121/ijsea.2014.5306.

Klaus Schwab, "The Fourth Industrial Revolution: What it Means, How to Respond", (January 2016)

Layne, K. & Lee, J. (2001) Developing fully functional e-government: a four-stage model, *Government Information Quarterly*, 18(2), 122-136

LYMEC, Press release – Young Liberal Leaders "European Liberal Youth asking for a single EU citizen number", Brussels, (October 2020)

Ministerial Declaration on eGovernment, the Tallinn Declaration, (October 2017)

National Interoperability Framework Observatory, Interoperability

Priisalu, J., Ottis, R. Personal control of privacy and data: Estonian experience. *Health Technol.* 7, 441–451 (2017)

Public key infrastructure, https://en.wikipedia.org/wiki/Public_key_infrastructure

Rabaiah, A., & Vandijck, E., (2009). A Strategic Framework of e-Government: Generic and Best Practice,

Rosner, M., Ritchie, H., "Technological Progress", (2013)

The Atlantic, "What Facebook Did to American Democracy", (October 2017)

The Conversation, "Digital Government isn't Working in the Developing World. Here's Why." (September 2018)

The New Yorker, "Estonia the Digital Republic", (December 2018)

United Nations, e-Government Survey, (July 2020)

World Bank, Access to Energy is at the Heart of Development, (April 2018)

World Economic Forum, "What is the Fourth Industrial Revolution?", (January 2016)

Yuval Noah Harari, "Sapiens: A Brief History of Humankind"

About the publishers

The **European Liberal Forum (ELF)** is the foundation of the European Liberal Democrats, the ALDE Party. ELF consists of several European think tanks, political foundations, and institutes and operates as an umbrella organisation for them. The foundation issues publications on Liberalism and European public policy issues and offers space for the discussion of European politics. ELF was founded in 2007 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks, and other experts.

The **European Liberal Youth (LYMEC)** is a pan-European youth organisation seeking to promote liberal values throughout the EU as the youth organisation of the ALDE Party and its parliamentary group in the European Parliament. LYMEC is made up of Member Organisations and Individual Members, and it is active across the breadth and diversity of the European continent. LYMEC's central aim is the creation of a liberal and federal Europe.

Published by the European Liberal Forum in cooperation with LYMEC-European Liberal Youth. Co-funded by the European Parliament.