

ECONOMICS AND DATA GOVERNANCE



The massive growth of data and data processing offers a considerable range of economic opportunities and opens up the possibility to endlessly expand our knowledge.

These developments have heightened the industrial, economic and commercial stakes and are creating a relentless global struggle for ownership and governance of data, and are likely to result in violations of fundamental rights and freedoms.



Soraya Duboc

is an engineer, former president of the Observatoire des Cadres (OdC) and a former member of the Ethics Committee for Agricultural Research. She is a member of the ESEC's Economic Activities Section, where she represents the CFDT group.

Contact:

soraya.duboc@lecese.fr
01 44 43 64 06



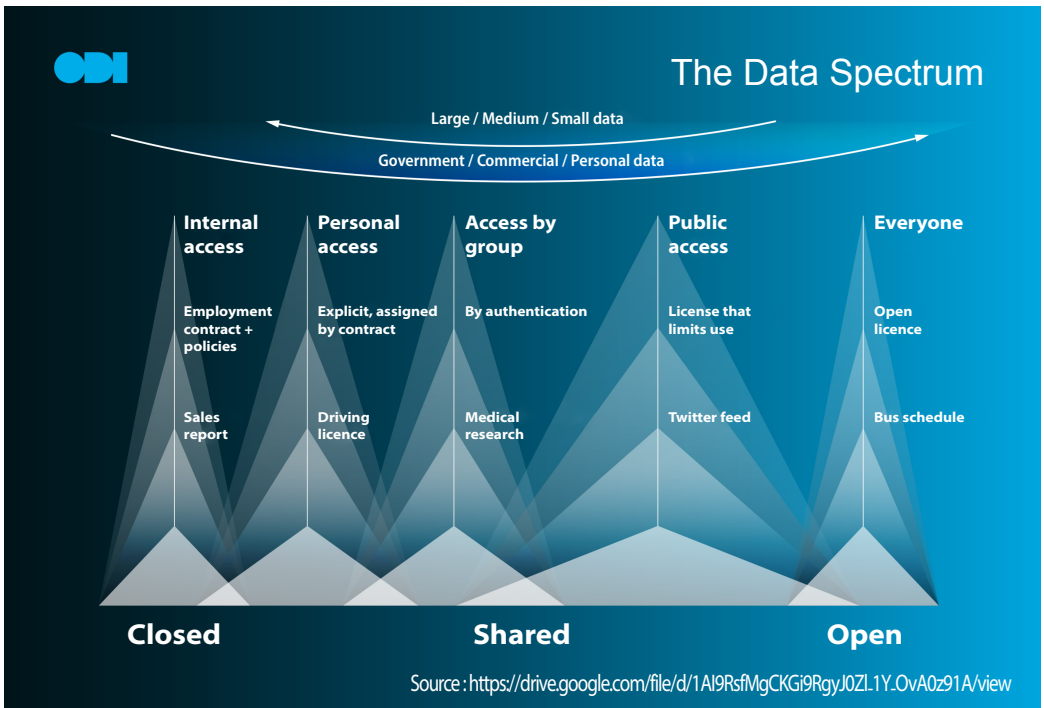
Daniel-Julien Noël

is a lawyer and former Chair of the Bar, and President of the National Chamber of Liberal Professions. He is a member of the ESEC's Economic Activities Section, where he represents the Liberal Professions Group.

Contact:

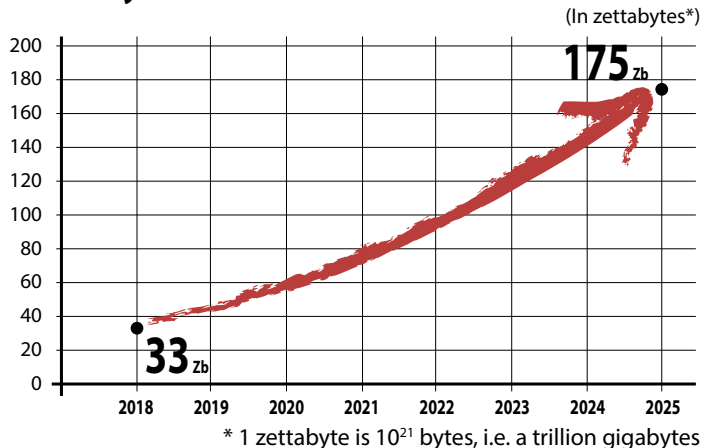
daniel-julien.noel@lecese.fr
01 44 43 64 30

How to make sense of the variety of data



Volume of data in the economy

The growing importance of data in the economy has led to a concomitant increase in the volumes exchanged, enabled by improvements in data networks (with the arrival of 5G) and the development of the Internet of Things. The European Commission has estimated that the global volume of data will increase by 530% by 2025, from 33 zettabytes in 2018 to 175 zettabytes in 2025.



Institutional and technological vulnerabilities

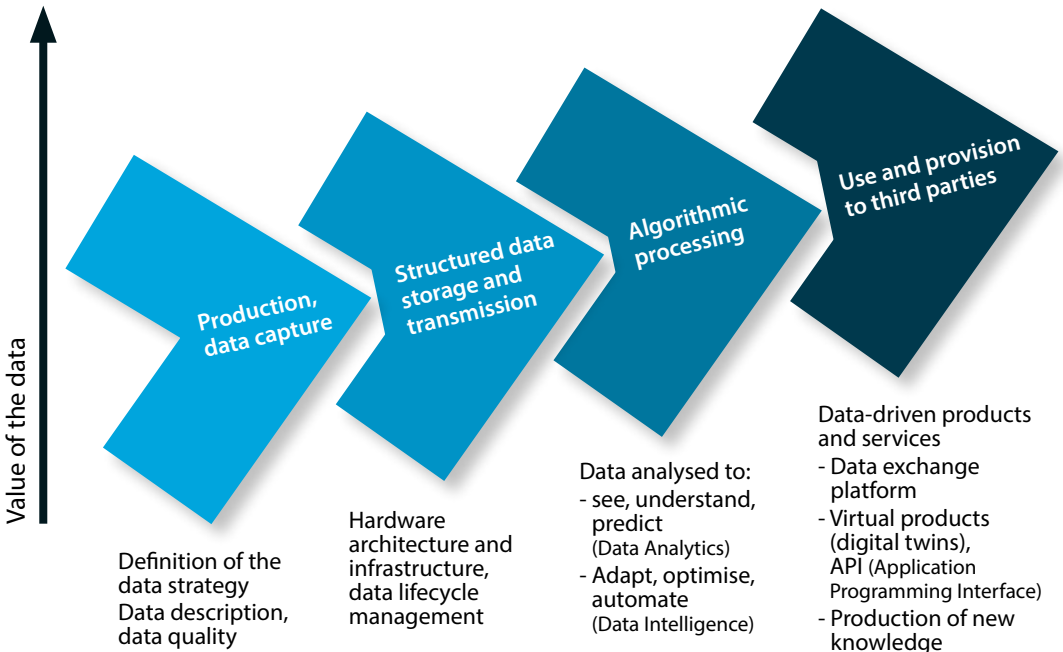
The data economy is growing. However, France, like the other EU Member States, is lagging behind; for example, current global data storage relies mainly on American and Chinese companies, which is now prompting European states to strengthen their sovereignty. European regulations are already in place and are being expanded. However, technological, economic and social vulnerabilities remain.

■ The data economy: recommendations to keep France in the race

The challenges of governing and regulating the data economy are numerous. First of all, governance needs to be consolidated, particularly at the international level, which raises questions about the extraterritoriality of foreign laws (the American Cloud Act) and the triple challenge of freedom, competition and security. Additionally, the “Net” giants are also taking on roles that were previously the province of states (the “Facebook Supreme Court”, Facebook’s “Libra” cryptocurrency). The ESEC therefore believes that legal and commercial regulation is needed and that citizens must be empowered to act.

The opinion supports the proposal for a three-year law to steer and monitor digital sovereignty in order to ensure rigorous management of investments and innovations, and finds that France has sufficient assets, but that they need to be strengthened through strong, accelerated cooperation within the European Union. We need to strengthen the educational, scientific and technical framework, and develop skills and qualifications essential to the data economy – including data processing, cybersecurity and storage infrastructure – while reinventing the economic, social and ethical framework.

■ Data Value Chain



Skills and resources needed along the data value chain

Strategic (what business model, what internal and external data?)

Organisational (data governance)

Managerial (cross-functional cooperation between business lines)

Technical resources and skills (technical infrastructure, data processing, cybersecurity, etc.)

THE ESEC'S RECOMMENDATIONS

- Recommendation 1: Use an encryption solution for sensitive data, whose code would be held by the customer and not by the technical intermediary, in order to protect data confidentiality.
- Recommendation 2: When US authorities request the transmission of personal data, require the consent of the individual concerned before sending the data.
- Recommendation 3: Require hosting companies to include specific clauses in their contracts, in order to make them legally responsible and thereby better protect users from unknowingly disclosing their personal data.
- Recommendation 4: Introduce a procedure to approve general terms and conditions of use (GTCs) at the national level, in order to verify their compatibility with positive law.
- Recommendation 5: Create a "Title V" in the Intellectual Property Code entitled "Right of Ownership over Personal Data", which would be supplemented by a public policy rule making personal data inalienable and non-transferable, in order to protect internet users.
- Recommendation 6: Adopt a three-year law to steer and monitor digital sovereignty in order to streamline the government's budgetary efforts and set guidelines for our digital strategy.
- Recommendation 7: Support the public data service in its effort to develop "data commons" by sharing public data and private data of public interest more widely.
- Recommendation 8: Establish an EU regulatory framework for artificial intelligence-based tools that is consistent with the principles of transparency, traceability and human control so that fundamental rights and freedoms are strengthened.
- Recommendation 9: Develop key skills for the future by increasing training for decision-makers on the strategic nature of digital data and by strengthening high-level academic research skills and qualifications.
- Recommendation 10: Work to prevent the poaching of useful skills in data processing and hardware infrastructure.
- Recommendation 11: In cooperation with other European partners, strengthen the choices made in strategic digital industries, including the development of data storage infrastructure.
- Recommendation 12: Strengthen cybersecurity skills in order to meet the needs of the data economy by diversifying training courses and increasing the number of people trained (initial and continuing training).
- Recommendation 13: Mobilise substantial resources to produce theoretical knowledge on data-driven business models and their challenges.
- Recommendation 14: Develop a data and digital intelligence culture within companies, in conjunction with the senior defence official; strengthen social dialogue to implement effective awareness-raising and information tools prior to the deployment of artificial intelligence tools; adapt cooperation and management methods.
- Recommendation 15: Make users aware of the risk of excessively consuming certain digital services, which are powerful harvesters of personal data.