Data, Digitalisation and Sector Resilience

Synthesis of a conference

Event organised by the Governance and Regulation Chair

Paris Dauphine-PSL University

Dauphine
CHAIRE GOUVERNANCE
ET RÉGULATION

Event organised by the Chair Governance and Regulation

April 15, 2026

Dauphine
CHAIRE GOUVERNANCE
ET RÉGULATION

Synthesis n°110
Paris Dauphine-PSL University

Data, Digitalisation and Sector Resilience

Speakers

Alexandre Abdalla-Araujo | National Water and Basic Sanitation Agency (ANA)

Arnaud Dietrich | French Energy Regulatory Commission (CRE)

Manuel Fernando Muñoz Quiroz | National Superintendency of Sanitation Services (SUNASS)

Annegret Groebel | Federal Network Agency (Bundesnetzagentur)

Ihor Mitroshyshev | National Energy and Utilities Regulatory Commission

Tomás de Oliveira Bredariol | International Methane Emissions Observatory (IMEO)

Giuseppa Ottimofiore | Head of the Effective Regulatory Delivery Programme, OECD of Regulatory Policy, OECD Public Governance

France Pégeot | Chair, OECD Network of Economic Regulators

Davide Stroppa | European Banking Authority (EBA)

Moderator

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Summary

This webinar was jointly organised by the Governance & Regulation Chair and the OECD.

Data and digital tools are rapidly redefining the landscape in which regulators operate. In sectors that are increasingly complex, interconnected and exposed to diverse risks—from climate disruptions to cyber threats—the ability to access, process and act on information in real time is becoming central to effective oversight. These technologies promise not only greater visibility over system performance, but also the possibility of anticipating vulnerabilities before they escalate into crises.

Yet this transformation is not without its challenges. The growing volume and variety of data raise fundamental questions about how regulators can integrate these resources into their decision-making processes. Turning raw data into meaningful insight requires not only technical capabilities, but also appropriate institutional frameworks, governance arrangements and a high degree of trust among stakeholders. Moreover, as regulatory environments become more dynamic, the pace at which information must be analysed and acted upon is accelerating.

Against this backdrop, this conference set out to examine how regulators are navigating this evolving terrain. It focuses on the role of data and digitalisation in strengthening sector resilience—understood not simply as the capacity to recover from shocks, but increasingly as the ability to anticipate, adapt and respond effectively to uncertainty. Particular attention is given to the practical use of tools such as early warning systems, stress testing and scenario analysis, as well as to the organisational and institutional conditions that enable their effective deployment.

A central thread running through the discussions is the shifting role of the regulator itself. As data becomes more integral to regulatory practice, institutions are required to develop new capabilities, rethink traditional approaches and engage more actively with a broader ecosystem of actors, including operators, governments, researchers and the public. This evolution raises important questions about capacity, coordination and the balance between innovation and control.

This report invites readers to explore these issues in greater depth. It offers insights into how regulatory communities are beginning to harness the potential of data and digital tools, while grappling with the complexities they introduce. In doing so, it provides a window into an area of regulatory practice that is likely to remain central in the years ahead.

Opening Remarks

Eric Brousseau | Scientific Director, Governance and Regulation Chair

On behalf of the President of Université Paris-Dauphine, I welcome all participants to the university. I am very pleased to resume our long-standing cooperation with the OECD, in particular with its Public Governance Directorate and the Network of Economic Regulators. For the past ten years, we have organised conferences in this room, and I am delighted to see you all here this morning for this event on data digitalisation and sector resilience. This conference forms part of a broader series of events exploring how regulators can leverage data to improve regulatory practices.

Data and digital tools are transforming how regulators monitor sectors, anticipate risks, and strengthen resilience. Access to real-time information, advanced analytics, and digital monitoring systems enables regulators to detect emerging vulnerabilities, test system robustness, and support more informed decision-making. However, to fully realise this potential, regulators face challenges in integrating data into regulatory processes and translating insights into effective action. These challenges are not only legal and technical but also relate to trust, which is essential when engaging multiple stakeholders. Today's event will explore how regulators across sectors use data and digital tools to enhance resilience, including through early warning systems, stress testing, and scenario analysis.

I now invite Giuseppa Ottimofiore to deliver the opening remarks.

Giuseppa Ottimofiore | Head of the Effective Regulatory Delivery Programme, OECD of Regulatory Policy, OECD Public Governance

We are delighted to resume and strengthen this collaboration with Université Paris-Dauphine, not only through this seminar but also through a broader series of webinars on the role of data and digitalisation in regulatory practice. I would also like to thank the organisers for hosting us in this excellent venue, which brings together regulators, academics, and practitioners.

Earlier this year, we held a webinar entitled Designing Data Sharing Arrangements: Institutional Choices for Regulators. Today's seminar is the second event in this series, which will continue at least until next spring. This topic is highly relevant across sectors represented in the Network of Economic Regulators, including energy, transport, telecommunications, and water. These systems are becoming increasingly complex and interconnected, while also being exposed to a growing range of risks, such as cyber incidents, climate-related disruptions, and supply chain shocks. Regulators are therefore expected not only to respond to these risks but also to anticipate them as early as possible.

Data and digitalisation play a crucial role in this context. They enable regulators to understand sector performance, assess whether policy objectives are being met, and make better intervention choices. What is changing significantly is the volume, quality, and speed of data, allowing signals to be detected much earlier. As a result, many regulators are moving from traditional periodic reporting towards continuous monitoring of performance.

This evolution creates important opportunities. For example, early warning mechanisms can help detect operational risks and emerging vulnerabilities at an earlier stage. It also supports more evidence-based decision-making and improves the ability to anticipate future developments and better support sectors.

However, challenges remain. Data is increasingly available from multiple sources, often in incompatible formats, and systems are not always interconnected. In addition, regulators require stronger analytical capacities and institutional processes to transform large volumes of data into meaningful insights. Without these elements, data alone will not lead to better regulatory decisions. The purpose of today's seminar is therefore to exchange not only theoretical perspectives but, above all, practical experiences across sectors, jurisdictions, and institutions. In particular, we will focus on the use of data for early warning systems, stress testing, scenario analysis, and strengthening institutional preparedness. I look forward to the discussions and thank all participants in advance.

Session 1 - Using Data as an Early Warning System

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Regulators increasingly rely on real-time and near-real-time data to identify emerging risks and anticipate disruptions. This session will explore how data systems, monitoring tools, and trend analysis can function as early warning mechanisms. Two speakers will present practical examples of how regulators use data and digital tools to detect vulnerabilities and raise awareness of potential risks.

How can regulators use data and digital tools to strengthen sector resilience?

Manuel Fernando Muñoz Quiroz | SUNASS

I will address a key question: how can regulators use data and digital tools to strengthen sector resilience? And I will answer it based on the experience of SUNASS, from the perspective of a water and sanitation regulator operating in a country where access gaps persist, cross-sectoral coordination remains fragmented, and institutional and financial resources are limited.

In this context, data and digital tools are not simply complementary to regulation; they are essential capacities. They enable us to anticipate risks, identify vulnerabilities, focus interventions, and strengthen sector resilience. Our innovation strategy is organised around two complementary dimensions. The first is internal innovation, which aims to strengthen how SUNASS operates. The second is external innovation, which aims to improve what regulation delivers to the sector.

This approach is implemented through two concrete instruments, both developed internally by SUNASS professionals: CION, which serves as a space for internal transformation, and CAMI YAKU, a national platform for the analysis and monitoring of drinking water information.

Building CAMI YAKU: from fragmented data to institutional capacity

To understand the need for CAMI YAKU, it is important to consider the context. Peru covers approximately 1.28 million square kilometres – the equivalent of France, Germany, Spain, and the United Kingdom combined – encompassing diverse geographical regions such as the Amazon, the Andes, and coastal areas. Before the introduction of CAMI YAKU, information was distributed across multiple areas, stored in fragmented databases, and often incomplete. The same information existed in different units but was not integrated.

In this situation, the challenge was not simply to build a better database, but to create an institutional capacity capable of generating timely and useful information for regulatory action. The name CAMI YAKU combines the concept of a monitoring centre with the Quechua word “yaku,” meaning water.

It operates from Lima and four macro-regional offices located in Piura, San Martín, Puno, and Arequipa. This distributed structure allows for closer proximity to the territory. Its outputs are organised across three levels:

- an immediate level, which includes real-time monitoring, early warnings, maps, and dashboards;
- a continuous level, focused on the development of applications and reports;
- a periodic level, associated with studies, special projects, and cooperation with other sector actors.

Monitoring service continuity and water quality

One of the most important questions for users in Peru is whether water will be available in their homes on a given day. Service continuity remains a major challenge and a significant public health risk, particularly for vulnerable populations who must store water when supply is interrupted. By 2025,

average service continuity had reached approximately 18 hours per day across 4.5 million connections. However, around 400,000 connections still received water for less than six hours per day.

In response, SUNASS developed an in-house monitoring system based on pressure and continuity sensors installed at 360 locations across the country. This remote and automated system generates early warnings and strengthens regulatory monitoring capacity.

Another important concern is whether the water supplied is safe. In many small cities, service providers either do not chlorinate water or do so inadequately. SUNASS addresses this issue through the MOREA system, which enables remote monitoring of chlorination. Twenty-six monitoring stations installed in reservoirs measure residual chlorine levels in real time. The data is transmitted remotely and shared with service providers. This has a significant effect: when providers know they are being monitored in real time, compliance improves. This demonstrates that data does not only measure performance; it also influences behaviour and strengthens regulatory effectiveness.

Improving transparency and communication with users

Another key issue for users is the lack of information during service interruptions. When systems fail, users often do not know when service will be restored. SUNASS has developed a monitoring system that identifies in real time the cause, location, duration, and population affected by each interruption. This system is complemented by YAKUNECTADOS, a bidirectional communication mechanism through which SUNASS interacts directly with users to verify whether service has been restored.

We have also developed YAKUMAP, an interactive tool that visualises access gaps and investment in water and sanitation across the country. It integrates information on service quality, coverage gaps, and the status of infrastructure projects. This tool enables regulators, policymakers, and citizens to understand both current conditions and future developments in the sector.

Impact on service providers and regulatory oversight

Finally, I would like to illustrate how these tools have transformed relationships between regulators and service providers. In the case of EPS Rioja, a service provider in the jungle region of Peru, monitoring of pressure and service continuity was previously entirely manual. With the implementation of CAMI YAKU, data collection has become automated, and information is now transmitted in real time, significantly improving monitoring and regulatory oversight.

With the implementation of CAMI YAKU, we now process the information collected and provide feedback to service providers, indicating precisely in which areas or sectors problems exist in the provision of water and sanitation services. This enables more targeted and effective interventions.

Internal transformation through CION

In addition to CAMI YAKU, we have developed CION as a centre for operational innovation on the internal side. As mentioned earlier, CION operates in three stages: first, process diagnosis and mapping; second, redesign and automation; and third, implementation with a focus on sustainability. Its objective is to reduce processing time, lower operational costs, and free up institutional capacity for analysis and decision-making.

One of the most significant outputs of CION is the “TRASS” system, a tribunal mechanism designed to resolve user complaints. This system processes approximately 60,000 case files per year. Previously, handling this volume of information required extensive time and effort. The redesigned system now extracts relevant information from complex case files, applies pre-structured legal criteria, and generates a draft resolution in approximately five minutes. Before the introduction of this system, the same process could take up to 35 days. The draft resolution is then reviewed and validated by a legal expert, who issues the final decision. This represents a substantial improvement in efficiency and responsiveness.

Building capacity, talent, and knowledge ecosystems

For us as a regulator, it is not sufficient merely to process data. It is equally important to promote awareness among younger generations—particularly university students—of the importance of water and sanitation services for society. For this reason, in 2025 SUNASS organised its first national data science competition. We received more than 270 applications, and the winning projects were implemented in four service providers. This initiative has since been expanded to the national level.

The "Data Zone" is not simply a competition; it is a strategic tool for attracting talent, building knowledge networks, and strengthening connections between the water sector, academia, and the technology community.

CAMI YAKU has also contributed to the production of valuable research outputs. In the second half of 2025, it supported studies on multidimensional poverty and access to drinking water, the relationship between water consumption and economic activity, and the issue of non-revenue water as a management challenge for service providers. These publications are openly accessible. For us, producing and disseminating such information is essential, as it allows academia and stakeholders to better understand the state of services across different regions of the country, not only through raw data but also through analytical research.

Conclusion: key lessons for regulatory resilience

To conclude, I would like to return to the central question: how can regulators use data and digital tools to strengthen sector resilience? Our experience suggests three key lessons.

- First, resilience requires visibility—regulators must be able to identify gaps, risks, and disruptions in a timely manner in order to act effectively.
- Second, data only creates public value when institutional capacities exist to translate it into concrete regulatory decisions and actions.
- Third, the efficiency of the regulator itself is an integral component of sector resilience; a more agile and focused institution is better equipped to respond to challenges affecting service quality and continuity.

Perhaps the most important lesson from our experience is that regulatory innovation does not depend solely on the availability of resources. It depends above all on the institutional capacity to prioritise, adapt, and develop solutions with a clear strategic purpose.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Thank you for this highly stimulating case study, which clearly demonstrates how improving transparency in a sector can influence the behaviour of service providers, making them more accountable not only to the regulator but also to the broader public. This is both insightful and encouraging.

In the interest of time, I will now turn to our second speaker, Tomas de Oliveira Bredariol. He oversees the analytical work of the International Methane Emissions Observatory and leads the OGMP 2.0 data analysis team. Prior to joining the United Nations Environment Programme, he worked at the International Energy Agency, where he led analysis on methane abatement and contributed to the development of the Global Methane Tracker. He began his career at the Brazilian Institute of Environment and Offshore Oil and Gas, focusing on risk management and emergency response.

Using Data and Satellites to Tackle Methane Emissions: The Methane Alert and Response System

Tomás de Oliveira Bredariol | IMEO

Meghan Demeter, Programme Manager for the Methane Alert and Response System, is unfortunately unable to attend, as she is participating in a regulatory network meeting organised by the International Energy Agency and the Climate and Clean Air Coalition, in coordination with the OECD Network of Energy Regulators.

This meeting is particularly significant, as it represents one of the first opportunities for regulators to engage in the development of methane emissions regulations. A key topic under discussion is precisely the Methane Alert and Response System, which I will now present.

The role of the International Methane Emissions Observatory

The International Methane Emissions Observatory, housed within the United Nations Environment Programme, was established in 2021 with support from the European Commission and other partners. Its mission is to provide actionable data on methane emissions to those who are in a position to act on it.

Methane emissions represent a major challenge, accounting for approximately 30% of global warming to date. At the same time, they offer one of the fastest opportunities to reduce temperature increases within our lifetimes. In many cases, particularly in the oil and gas sector, mitigation is cost-effective. However, action has been limited due to a lack of information—methane is neither visible nor detectable by smell, making it difficult to monitor without appropriate tools.

The Observatory addresses this gap by identifying key sources of methane emissions and providing this information to regulators, operators, investors, and other stakeholders. One of its core initiatives is the Methane Alert and Response System (MARS).

The Methane Alert and Response System's functioning

The system operates in several stages.

First, it detects methane emissions and attributes them to specific facilities. This is achieved using data from approximately 35 satellites and sensors, which identify large methane emissions—typically above 100 kilograms per hour, the current detection threshold for satellite systems. Although many emissions fall below this threshold, thousands of detectable plumes are identified, each representing a significant opportunity for mitigation. Methane detection is not only relevant for environmental protection but also for operational efficiency and safety, as methane constitutes approximately 90% of natural gas.

The second stage involves notifying relevant stakeholders, including governments, in-country representatives of the United Nations Environment Programme, and companies participating in the Oil and Gas Methane Partnership 2.0.

The third stage focuses on response. This involves following up with stakeholders to determine what actions have been taken, whether emissions have ceased, and whether additional technical or institutional support is required. The final stage consists of ongoing monitoring to assess how emissions evolve over time and to ensure that mitigation measures have been effective.

Satellite technology and data processing

The system furthermore relies on a constellation of satellite technologies, including both targeted "point source imagers," which focus on specific facilities, and "area flux mappers," which provide regular global coverage. For example, the Sentinel-5P satellite, operated by the European Space

Agency, monitors emissions across the globe every few days.

In practice, the system identifies emission sources across key sectors such as oil and gas, coal, and waste management. Analysts use machine learning and artificial intelligence to screen satellite data, cross-reference it with wind patterns and other information, and then validate findings through expert review. This ensures the accuracy and reliability of detected emission events.

A distinguishing feature of the Methane Alert and Response System is its integration of multiple data sources, including both publicly available data and information provided by partners. This data is then shared free of charge with stakeholders worldwide. Regional case managers help ensure that alerts reach the appropriate actors, facilitating timely and effective responses.

Early results and real-world impact

We are already observing tangible results. In more than ten countries, notifications have led to concrete actions, such as repairing leaks, closing malfunctioning wells, or reactivating flaring systems. These interventions have resulted in the rapid cessation of emissions in affected areas.

However, significant challenges remain. When the system was launched in 2024, it operated in a prototype phase and received responses to only 1% of notifications. By 2025, this had improved to 12%, which is encouraging progress. Nevertheless, nearly 90% of notifications still receive no response, meaning that while information is delivered, follow-up action is not always reported or undertaken.

We observe that, in many cases, there is still no follow-up indicating whether mitigation measures have been implemented in response to the notifications we issue. In some instances, this is linked to issues of data sharing and confidentiality. However, there remains significant potential to increase response rates and, consequently, the number of mitigation actions undertaken.

Each detected super-emitting event represents a major opportunity for climate action. In many cases, mitigation is cost-effective and can also contribute to improved energy security. We therefore aim to further increase response rates and accelerate the reduction of methane emissions. Thank you very much. I would be happy to answer any questions.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Thank you for this stimulating case study, which illustrates that data collection not only helps identify where problems occur but also enables targeted interventions and assistance. Although this example relates to environmental issues at a global scale, the same logic applies to other sectors, such as water management, where identifying leaks and supporting local operators is equally essential.

Discussion

From the floor

I work at the Australian Competition and Consumer Commission. Could you clarify the nature of the methane emissions you detect? Are you primarily identifying operational irregularities—such as temporary malfunctions—or long-term, continuous emissions? Or does the system address both types?

Tomás de Oliveira Bredariol | IMEO

We address both types of emissions. We have identified sources that have been emitting methane for decades, including malfunctioning flares or intentional venting where operators lack infrastructure to bring gas to market. In such cases, emissions may be continuous.

The most common situation varies by sector. In coal mining, for example, methane is often vented through ventilation shafts for safety reasons. While mitigation technologies exist, such as regenerative thermal oxidisers, they are not widely implemented, and emissions remain ongoing. Similarly, landfills can produce long-term methane emissions if not properly managed. In the oil and gas sector, the situation is more nuanced. There are both intentional emissions—for example, during maintenance operations—and unintentional emissions caused by equipment malfunctions or leaks. Based on our observations, many super-emitting events we detect are planned, non-routine operations, and several others result from unintended leaks or failures.

From the floor

What motivates operators to address methane emissions? Do incentives vary by country—for example, through regulatory requirements, fines, or emissions trading mechanisms—or do you simply provide information for countries to act upon within their own frameworks?

Tomás de Oliveira Bredariol | IMEO

Our role is limited to providing information; we do not have enforcement powers. Regulatory frameworks vary significantly by country. In some jurisdictions, regulations prohibit such emissions, and operators may face fines or mandatory remediation requirements.

In many cases—particularly for unintentional emissions—operators act once they are informed, as reducing methane leakage can generate financial benefits by preserving saleable gas. In other cases, such as malfunctioning flares, reputational considerations play a significant role, especially for large companies.

However, in sectors such as coal mining and landfill management, where regulatory frameworks may be weaker or absent, mitigation often depends on external incentives. Without such incentives, action is less likely to occur.

From the floor

I work at the Portuguese Telecommunications Regulator and I would like to raise a question regarding data management. In Portugal, we are currently implementing a new subsea cable connecting the mainland with two islands. This cable will include external sensors designed to provide early warning for tsunamis. However, these sensors capture a wide range of data, including information unrelated to their primary purpose—for example, detecting marine life such as whales. This raises concerns about how to manage such data securely while maintaining the effectiveness of the early warning system. Delays in data validation—for example, requiring approval from defence authorities—could reduce the effectiveness of the system.

Given that your work relies on satellite data with similarly broad observational capabilities, do you face

comparable challenges? If so, how do you address them?

Manuel Fernando Muñoz Quiroz | SUNASS

In Peru, we have limited experience with satellite-based monitoring, as we currently operate only one satellite, primarily used for educational purposes in remote areas. However, I agree that satellite technology could play a significant role in monitoring national conditions, including environmental issues such as water contamination.

In the water and sanitation sector, we currently rely more on drones to monitor urban areas, particularly when addressing river pollution. Nevertheless, there is clear potential to expand the use of advanced technologies, including satellites, across the country. This is an area we need to further develop.

From the floor

Allow me to briefly comment on the broader concept of resilience. The example discussed today illustrates what can be described as "proactive resilience," a concept that has gained prominence since the COVID-19 crisis. This approach goes beyond simply restoring systems to their pre-crisis state; it seeks to improve them. In this context, training and education are essential components of resilience-building, and I would like to emphasise their importance.

From the floor

I represent the Commission for Communications Regulation of Ireland, and I have two brief questions. First, for Manuel: regarding the MOREA system, you mentioned the use of WhatsApp notifications related to chlorination levels. Are these notifications directed at operational teams responsible for maintenance, or are they used as a public warning system for citizens?

Second, for Thomas: in cases where competent authorities have enforcement powers, do you engage directly with these authorities, or do you limit your communication to operators?

Manuel Fernando Muñoz Quiroz | SUNASS

In Peru, we face significant challenges in rural areas, where there are approximately 27,000 small service providers. In many of these areas, chlorination is either not performed or performed inadequately, often due to manual processes and misconceptions about water quality.

The MOREA system is designed primarily as a monitoring and alert tool for regulatory and operational purposes. It allows us to track chlorination levels in real time and identify when chlorination is not being carried out as required. Alerts are sent to the relevant public authorities and operators to prompt corrective action. At this stage, it is not used as a direct public warning system, although it has the potential to be expanded in the future.

Tomás de Oliveira Bredariol | IMEO

We operate with a tiered notification system. Our first priority is to inform designated national focal points—competent authorities identified by governments. Currently, we collaborate with approximately 20 countries in this framework.

The second level of notification targets operators participating in the Oil and Gas Methane Partnership 2.0, who receive alerts shortly after the authorities. In cases where neither a competent authority nor an operator can be clearly identified, we rely on UNEP in-country representatives.

Session 2 - Strengthening Resilience Through Stress Testing and Scenarios

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Stress testing and scenario analysis are increasingly used by regulators to assess how sectors respond to shocks and disruptions. These approaches rely on data and digital tools to anticipate risks, identify vulnerabilities, and inform response strategies. This session will explore how different sectors apply these methods to strengthen resilience. Our first speaker is Davide Stroppa, Senior Policy Expert and Team Leader for AI Act Implementation in the Digital Finance Unit of the European Banking Authority.

Digital resilience in the financial sector: regulation, data and supervisory agility

Davide Stroppa | EBA

Digitalisation has fundamentally transformed financial services over the past decade, reshaping the risk landscape at an unprecedented pace. While it creates significant opportunities, it also amplifies operational risks and increases systemic interconnectedness. For this reason, digital resilience has become a strategic priority for both financial institutions and supervisors.

I will structure my remarks around three key dimensions:

- how regulation in the European Union addresses resilience challenges, particularly those related to cyber risk;
- how knowledge and data contribute to effective supervision and resilience;
- how supervisory responsiveness and timeliness have become critical components of resilience.

Digitalisation and the operational resilience challenge: the role of DORA (Digital Operational Resilience Act)

Let me begin with the impact of digitalisation on operational resilience. Financial services today depend heavily on ICT systems, cloud infrastructure, APIs, and third-party providers. While these dependencies enable innovation and efficiency, they also create new vulnerabilities. A disruption in one component can cascade across the system, turning a localised operational issue into a broader financial stability concern.

In response, the European Union introduced the Digital Operational Resilience Act (DORA), which started applying in January 2025. The main novelty of DORA is that it is not simply another regulation adding to the existing rulebook; instead, it establishes a comprehensive and harmonised framework for digital operational resilience across the entire financial system, including banks, insurers, and asset managers.

This framework is built on five key pillars:

- First, it strengthens ICT risk management, requiring financial entities to adopt robust governance, clear responsibilities, and effective controls to identify and mitigate risks;
- Second, it introduces a harmonised incident reporting regime, which is particularly important given the speed of propagation and cross-sectoral nature of ICT incidents;
- Third, it places strong emphasis on digital operational resilience testing, including advanced testing, to assess that systems are not only compliant in theory but effective in practice.

- Fourth, it lays out a set of principle-based rules to guide financial entities when monitoring risks arising from functions outsourced to ICT third-party service providers
- Finally, it introduces an EU-wide oversight framework for critical providers of ICT services, to be carried out by the three European supervisory authorities (ESAs -EBA, ESMA, and EIOPA).

Data as the foundation of supervisory knowledge

The second dimension of resilience is knowledge, which starts with data.

This is clearly exemplified by the information that supervisors and the ESAs collect on major ICT incidents. Financial entities are required to report ICT incidents to national authorities, which in turn share this information with the three ESAs and provide supervisory feedback to financial entities.

First, high-quality, timely data enables national supervisors to identify vulnerabilities, detect patterns, and distinguish between isolated incidents and systemic issues. Moreover, this information can then be fed back into supervisory actions. Second, at the European level, aggregating data across all Member States allows the ESAs to "connect the dots" and identify trends, sector-specific risks, or emerging threats.

However, data alone are not sufficient. In a fast-moving environment, timely sharing of information is critical, as delays in communication can significantly worsen the impact of an incident.

This is particularly true for cyber crisis, which are inherently cross-border, thus necessitating coordinated responses. To address this, the European Systemic Cyber Risk Coordination Framework (EU-SCICF) has been established to facilitate cooperation among supervisory authorities across sectors. This framework does not replace existing crisis management structures but aims to connect them, ensuring that relevant actors have a shared understanding of the situation as it unfolds, and can respond in a coherent manner.

Supervisory responsiveness in a real-time financial system

The third dimension is time, or supervisory responsiveness. Digitalisation implies that banking has become a fast-moving environment, for instance, making deposits more volatile as they can move faster than in the past. Therefore, both banks and supervisors need plans to react quickly.

In this context, supervisory technology—commonly referred to as "SupTech"—plays a critical role. These tools enable more efficient data management, advanced analytics, and faster identification of risks. They allow supervisors to process large volumes of data, detect anomalies, and identify early warning signals that might otherwise go unnoticed. Importantly, these tools do not replace human judgement but enhance it, enabling supervisors to focus their expertise where it is most needed.

For example, the EBA is currently developing a tool to monitor stablecoins in real time. This is particularly relevant as we are talking about activities and actors that are inherently digital and fast moving, where traditional supervisory approaches alone may not be sufficient in such an environment. Similar applications exist in areas such as anti-money laundering, counter-terrorism financing, market surveillance, and data quality assurance.

Conclusion: a shared responsibility for resilience

In conclusion, digitalisation has fundamentally changed the nature of operational risk in the financial sector. The DORA framework provides a robust and harmonised response to these challenges. At the same time, resilience depends on high-quality data, effective coordination, and the ability of authorities to act quickly. Ultimately, operational resilience is a shared responsibility: financial institutions must strengthen their own capabilities, while supervisory authorities must become more agile, data-driven, and responsive.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Thank you, Davide, for this precise and insightful presentation, delivered perfectly within the allotted time. While the financial sector has its specific characteristics, many of the challenges you described are equally relevant to network industries such as energy and transport, where digitalisation also introduces new risks and dependencies.

I now have the pleasure of introducing our second speaker for this session, Annegret Groebel. She works at the German Federal Network Agency, the Bundesnetzagentur, which regulates electricity, gas, telecommunications, postal services, and railways. She has served as President of the Council of European Energy Regulators since 2019 and as Vice-Chair of the International Confederation of Energy Regulators since 2020. She brings extensive experience in regulatory reform and sector-specific regulation.

Strengthening Systemic Resilience: Digital Platforms and Energy Security in Practice

Annegret Groebel | Bundesnetzagentur

I will present two examples illustrating the use of digital tools to strengthen resilience. The first concerns our preparations for the snap parliamentary elections in Germany in February 2025, in our capacity as Digital Services Coordinator. The second relates to scenario modelling for gas supply during winter, in response to the recent energy crisis.

Case Study: Germany's 2025 Snap Elections

The role of the Digital Services Coordinator

The role of the Digital Services Coordinator, assigned to certain telecommunications regulators, involves coordinating all stakeholders operating within the framework of the Digital Services Act. While we do not directly regulate online platforms, we are responsible for ensuring coordination among relevant actors.

A particular focus is placed on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), which are supervised directly by the European Commission, with support from national coordinators. These entities are defined as platforms with more than 45 million users within the European Union. Due to their scale, they are subject to specific obligations related to systemic risks arising from their digital systems, including algorithms and content distribution mechanisms.

Systemic risks under the Digital Services Act

In preparation for the elections, we conducted stress testing exercises to ensure that these platforms had implemented appropriate mitigation measures. The objective was to prevent negative impacts on the electoral process, such as manipulation or disinformation.

Under the Digital Services Act, these platforms are required to conduct annual risk assessments, identifying potential negative effects on public discourse, electoral integrity, and public security. This reflects a broader shift in recognising digital platforms as critical infrastructure, comparable in importance to traditional network systems.

There is a clear parallel between systemic risks in digital platforms and those observed in traditional infrastructure sectors. In the context of the Digital Services Act, systemic risks are closely linked to the design and functioning of platforms' recommender systems, advertising mechanisms—particularly political advertising—and the potential for intentional manipulation of services. This includes inauthentic behaviour, automated exploitation of platforms, and coordinated disinformation campaigns.

These risks are further amplified by algorithmic systems and, increasingly, by artificial intelligence, which can accelerate the rapid and wide dissemination of illegal or misleading content. As a result, platforms are required not only to assess these risks but also to implement additional safeguards to

prevent negative impacts on democratic processes, particularly elections.

Mitigation measures and regulatory approach

Once risks have been identified, platforms must take a range of mitigation measures. These include adapting the design and functionality of their services and interfaces, strengthening content moderation processes, and testing and adjusting their algorithmic systems, including recommender systems. They must also reinforce internal processes for detecting systemic risks, conduct testing, and document their actions to ensure accountability and enable effective supervision.

In addition, platforms are required to implement external measures, such as awareness-raising initiatives, and to ensure that information presented to users is authentic and accurately displayed. Given the complexity of these systems, the Digital Services Act adopts an approach that combines elements of self-assessment with regulatory oversight. Platforms are responsible for identifying their own risks and implementing appropriate measures, but supervisory authorities—particularly the European Commission—retain the power to investigate and sanction non-compliance.

A key feature of this framework is that regulators do not prescribe specific technical solutions. Instead, platforms must demonstrate that their measures are proportionate and effective in addressing identified risks. To support this, researchers may be granted access to relevant data in order to independently assess the adequacy of these measures. This reflects the practical reality that regulators cannot fully determine the most appropriate solutions for highly complex digital systems.

The concept of systemic risk in this context refers to the potential breakdown of an entire system, rather than isolated components. Moreover, when such systems occupy a central position within a broader ecosystem, their failure can have cascading effects across other sectors. This creates what may be described as a "double systemic risk," extending beyond the immediate domain of digital platforms.

In application: Germany in 2025

Turning to the practical implementation of these principles, I will describe our experience as Digital Services Coordinator in Germany during the snap parliamentary elections of February 2025. The timeframe was extremely limited: the government collapsed in early November, was formally dissolved at the end of December, and elections were held on 23 February, leaving less than three and a half months for preparation.

In response, we immediately established an internal election task force. We coordinated closely with all relevant stakeholders, including the Ministry of the Interior, electoral authorities, regulatory bodies, and, crucially, the very large online platforms and search engines. We also conducted public awareness campaigns to inform voters about risks such as foreign information manipulation and disinformation.

On 24 January, we organised a roundtable with the six largest platforms. On 31 January, we conducted stress testing exercises to verify whether the required mitigation measures were effectively implemented. In parallel, we established a dedicated incident response structure, including a 24/7 hotline, operational for three weeks before, during, and after the election. This ensured that any reported incidents could be addressed immediately.

Scenario Modelling in Response to the Energy Crisis

Stress testing and lessons learned

The stress testing itself was based on simulated scenarios, including disinformation campaigns, fake accounts, and the use of artificial intelligence—such as deepfakes—to influence the electoral process. Platforms were required to respond to these scenarios in real time, demonstrating their mitigation measures and reporting mechanisms. The exercise involved multiple stakeholders, including major platforms such as Google, LinkedIn, Microsoft, Meta, Snapchat, TikTok, and X, as well as national

authorities, civil society organisations, and researchers.

The objective was to ensure that all required safeguards were in place and that communication channels between stakeholders functioned effectively, thereby strengthening the resilience of the electoral process.

Following the elections, we conducted an ex-post evaluation. While no major incidents occurred, we identified certain shortcomings and reported potential infringements to the European Commission for further investigation. One key lesson was the importance of preparedness, particularly in ensuring effective incident reporting and documentation. Another critical issue was the timeliness of access to platform data for researchers. Although such access is legally guaranteed, delays reduced its effectiveness, highlighting the need for improved data interfaces and accessibility.

Scenario modelling for gas supply security

The second example is more traditional in nature and relates to scenario modelling for gas supply security. This exercise was prompted by the disruption of Russian gas supplies in 2022, following the invasion of Ukraine and damage to the Nord Stream pipeline. In such a scenario, the Bundesnetzagentur would be responsible for allocating limited gas supplies, prioritising households and critical infrastructure. To prepare for this possibility, we developed a model simulating the German gas system, including all entry and exit points. The model was updated in November 2023 for the winter period through March 2024. It incorporated assumptions on consumption based on historical data, including the impact of particularly cold years, as well as assumptions regarding LNG terminal utilisation and cross-border gas flows.

We then conducted scenario analyses. Some scenarios assumed reduced consumption, while others assumed higher demand, increased exports, or reduced imports. These simulations allowed us to assess potential storage levels and identify conditions under which supply deficits might occur.

Findings and implications for preparedness

The results showed that in most scenarios, supply remained sufficient, although storage levels declined. However, in two scenarios—characterised by high demand and reduced supply—critical shortages could occur by early February, with storage levels falling to minimal thresholds. While increased LNG utilisation could mitigate these risks, this relied on optimistic assumptions.

This modelling exercise demonstrated both the fragility of the system under certain conditions and the importance of preparedness. It also enabled us to identify potential mitigation measures in advance, thereby enhancing our capacity to respond effectively in the event of a crisis.

Conclusion: managing endogenous and exogenous risks

In conclusion, these two examples illustrate different types of systemic risk. In the case of digital platforms, risks are endogenous, arising from the design and operation of the systems themselves. In the case of gas supply, risks are exogenous, resulting from external shocks. In both cases, regulatory action involves ensuring preparedness, conducting stress testing, and implementing appropriate mitigation measures to strengthen resilience.

In both cases I have presented, the objective of stress testing and scenario analysis is to ensure that the responsiveness of key actors is sufficient to minimise the impact of disruptions. In the case of digital platforms, this means protecting the integrity of the electoral process and preventing manipulation, including foreign interference. In the case of gas supply, it involves forecasting potential shortages, preparing crisis management structures, and avoiding worst-case outcomes. A critical aspect in both contexts is crisis communication. It is essential to strike a balance: on the one hand, avoiding the creation of a self-fulfilling prophecy by overstating risks; on the other hand, ensuring that stakeholders understand the need for preparedness, particularly in situations where supply is no longer guaranteed.

The follow-up processes differ depending on the context. In the case of digital platforms, follow-up actions are primarily directed at improving the mitigation measures implemented by large platforms, based on ex-post evaluations. In the gas sector, follow-up measures are more structural and long-term. These include reducing dependency on fossil gas, increasing the use of renewable energy, improving storage capacities, and diversifying energy sources. These measures go beyond immediate crisis management and contribute to long-term system resilience.

Davide Stroppa | EBA

I would highlight how the two types of stress testing you described closely resemble approaches used in the financial sector. The gas supply scenario represents an exogenous shock, where a macro-level disruption is applied to the system. In financial stress testing, we similarly apply macroeconomic scenarios to a sample of major banks—typically around 65 institutions representing approximately 75% of total assets—and assess the impact on their balance sheets. The results are then used by supervisors to guide their actions and communication.

The second example, involving digital platforms, reflects a more endogenous approach. Here, the focus is on whether adequate mitigation measures are in place and on learning from simulated scenarios. This is comparable to recent cyber resilience stress tests conducted by central banks, where simulated cyberattacks are used to assess institutions' preparedness, governance, and response mechanisms. The objective is not only to test systems but also to derive lessons for improvement.

Despite differences between sectors, the structure and purpose of stress testing are similar. This highlights the value of cross-sectoral exchanges such as this one.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Thank you, Davide. Your comment illustrates precisely the purpose of this seminar: to share regulatory practices across sectors and identify common approaches that can inspire innovation elsewhere.

Session 3 - Building Institutional Preparedness

Eric Brousseau | Scientific Director, Governance and Regulation Chair

Strengthening sector resilience requires not only data and analytical tools but also institutional capacity to act under uncertainty with speed, decisiveness, and coordination among stakeholders. This panel will explore how regulators develop organisational preparedness, anticipate risks, manage crises, and ensure resilient service delivery in complex and rapidly evolving environments.

From Data to Resilience: Preparing Energy Regulators for a Digital Future

Arnaud Dietrich | CRE

Institutional preparedness in the context of digitalisation is a critical issue because data and digital technologies are no longer merely tools for regulators—they form the operational foundation of our work. Like any critical infrastructure, this foundation must be resilient, secure, and adaptable to current and future challenges.

At the Commission de régulation de l'énergie, we are responsible for regulating electricity and gas networks, ensuring the proper functioning of energy markets, managing support schemes for renewable energy, and informing public debate on energy issues. We are a relatively small organisation, with approximately 160 staff and an annual budget of €24 million.

Digitalisation is profoundly reshaping energy markets. Between 2020 and 2025, the volume of orders and transactions monitored by the CRE increased from 10 million to 250 million per month—a 25-fold increase. This growth enhances market liquidity but also increases the risk of manipulation and operational failures, which are more difficult to detect.

For the CRE, this has required a complete transformation of our tools and infrastructure. Data storage and processing capacities have increased tenfold, and our surveillance algorithms have been adapted to analyse these large volumes of transactions. In 2024 alone, we analysed more than 15 million transactions, representing €180 billion. This operational reality highlights a fundamental principle: without mastery of data, effective regulation is impossible. To ensure security and resilience, we have pursued advanced cybersecurity measures and became the first French regulator to achieve certification under the NIS2 directive at the highest level.

This certification required the implementation of more than 100 measures, including dynamic risk analysis, intrusion detection systems, server redundancy, and continuous monitoring using certified tools approved by the national cybersecurity authority. We also established an internal cybersecurity culture through a dedicated committee involving all departments.

For a small organisation, this represents a significant investment—approximately 18 months of work and substantial human and technical resources. However, this effort is essential. As regulators, we must lead by example: if we require operators to secure their infrastructures, we must ensure our own systems meet the highest standards.

In conclusion, I would highlight three key messages. First, digitalisation increases both transparency and complexity in markets. Second, data is a strategic asset and must be central to regulatory action. Third, institutional preparedness is essential but comes at a cost, requiring prioritisation, investment, training, and cooperation with other regulators.

Ultimately, regulators must move beyond reactive approaches and anticipate future challenges. Embedding digital resilience into our organisational DNA is therefore critical.

From Disaster to Resilience: Coordinated Governance After the Rio Grande do Sul Floods

Alexandre Abdalla-Araujo | ANA

I will present our institutional response to the 2024 floods in Rio Grande do Sul, one of the most severe hydrological disasters in Brazil's history.

This event constituted a true institutional stress test. The region experienced unprecedented rainfall—over 700 millimetres within ten days—affecting 478 municipalities and 2.4 million people, resulting in 108 fatalities and 27 missing persons.

In response, the National Water and Basic Sanitation Agency established a permanent technical advisory group, involving approximately 15 organisations, including government agencies, universities, and research centres. This was not a temporary task force, but a structural mechanism designed to strengthen resilience through coordinated action.

Our objective was to create a unified technical foundation, transforming data into actionable insights for sustainable and resilient systems. This approach is based on three pillars.

The first pillar is a shared diagnostic framework, providing a common technical baseline. For example, we reconstructed the flood using hydrodynamic models, identifying critical factors such as a rapid 20-metre rise in water levels in certain rivers, which contributed significantly to the disaster.

The second pillar involves translating scientific knowledge into policy-relevant decisions. We updated key hydrological parameters, such as intensity-duration-frequency curves, incorporating data from the 2024 event. This revealed that events previously considered to occur once every 100 years may now occur every 77 years in some regions. Climate projections further indicate that by 2100, the intensity of such events could increase by 20%, with frequency potentially multiplying by five. These updated parameters are now mandatory for projects seeking federal funding.

The third pillar is multi-level coordination, with the agency acting as a central technical anchor to align stakeholders and ensure coherent responses.

Through the third pillar—multi-level coordination led by ANA—we have established effective communication channels across different sectors of society. This enables the sharing of relevant information, protocols, and guidelines, contributing to the development of a more sustainable and resilient future.

In conclusion, ANA is building resilience through collaboration among multiple partners, grounded in a unified technical framework. The Technical Advisory Group has created synergies with other ANA initiatives, supporting reconstruction efforts while strengthening permanent institutional capacity. In essence, data enables preparedness, but governance ensures its effectiveness.

Data-Driven Regulation Under Crisis: Ukraine's Electricity Sector Experience

Ihor Mitroshyshev | National Energy and Utilities Regulatory Commission

I will briefly present Ukraine's experience with digitalisation and data-driven regulatory management in the electricity sector.

Our information system is designed to collect, process, and analyse electricity market data in order to support regulatory decision-making. It integrates multiple data sources, including transmission system operators, market operators, power exchanges, energy buyers, and neighbouring systems.

On a daily basis, we process more than 40 standardised datasets. These data are validated, cleaned, stored, and then used to generate analytical dashboards and reports. Currently, the system manages

over 200 gigabytes of data across 35 databases and provides approximately 180 dashboards and analytical tools for both internal and external users. This infrastructure enables continuous monitoring of the electricity market and allows us to respond rapidly to emerging challenges. It provides decision-makers with comprehensive and up-to-date insights into the functioning of the energy system.

The system was developed in 2019, following the introduction of a competitive electricity market in Ukraine. Since then, we have continuously expanded our data sources, including direct data requests from market participants and information from neighbouring transmission system operators. In recent years, however, we have faced unprecedented challenges due to the war in Ukraine. These include infrastructure damage, power outages, and disruptions to data flows. Despite these conditions, our system has remained operational and has played a critical role in supporting regulatory decisions.

Let me illustrate this with two examples.

The first concerns renewable energy. Following market liberalisation, renewable generation expanded rapidly, but this led to increasing curtailment due to system constraints. Using our data analytics, we identified the scale and causes of this issue. Based on these insights, we introduced regulatory changes, including the recognition of energy storage as a separate market activity. This led to a significant increase in storage capacity, a reduction in curtailment events, and a decrease of more than 50% in renewable energy curtailment compared to 2022.

The second example relates to emergency situations caused by wartime damage. Since February 2022, Ukraine has experienced repeated attacks on energy infrastructure, including generation facilities and transmission networks. These attacks have resulted in sudden losses of generation capacity and created severe imbalances in the electricity market.

Our system allowed us to analyse these disruptions in real time. Based on this analysis, we introduced emergency regulatory measures to protect market participants from unpredictable financial losses. These measures included the temporary suspension of market operations, the suspension of bilateral contracts, and the use of average daily market prices for settlements.

This approach helped stabilise the market and protect participants during repeated crisis situations. These examples demonstrate that data-driven systems are essential not only for effective regulation but also for crisis management in the energy sector. Looking ahead, we consider digitalisation a long-term strategic priority. We plan to further expand our system, improve data quality, and introduce new analytical tools to enhance transparency, resilience, and sustainability, even under extreme conditions.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

These presentations clearly show that climate change and geopolitical instability are major sources of stress for regulated sectors. In this context, resilience requires not only data sharing but also the adaptation of governance systems to anticipate and manage crises effectively. I now open the floor for questions.

Discussion

From the floor

Given the current geopolitical situation in the Middle East, are you planning to update your procedures, as you did, following the Russian invasion of Ukraine?

Annegret Groebel | Bundesnetzagentur

We currently maintain a monitoring dashboard that tracks key indicators such as prices and storage levels, ensuring transparency. However, we have not yet updated our modelling framework, as the current situation differs from the crisis of 2022–2023.

While prices have increased, they have not reached the levels observed during the previous crisis. Moreover, we are now better prepared, having diversified our energy supply sources and reduced dependency on single providers. At present, the main challenge relates to pricing and affordability rather than supply security. Nevertheless, the situation remains dependent on geopolitical developments.

From the floor

I work for the Canada Energy Regulator. About cybersecurity and data sharing, how do you engage with companies regarding the reporting of incidents, particularly given concerns about confidentiality? What requirements exist under frameworks such as NIS2?

Arnaud Dietrich | CRE

The NIS2 directive establishes cybersecurity requirements for regulators and critical infrastructure operators. Although the directive has not yet been fully transposed into French law, we have implemented its principles and obtained a high-level certification.

Cybersecurity incidents occur regularly, although most are minor. For this reason, communication about incidents is handled carefully. However, we have established comprehensive crisis management procedures, including recovery plans, communication strategies, and dedicated response teams.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

In France, a national cybersecurity agency oversees the implementation of cybersecurity requirements across sectors and coordinates with regulators. There is a division of responsibilities: sector regulators focus on prevention, while specialised agencies handle incident response and the protection of critical digital infrastructure.

From the floor

As a member of the French National Cybersecurity Authority, I would like to clarify that incident response is primarily handled by the national cybersecurity authority, as well as regional and national Computer Security Incident Response Teams (CSIRTs). Regarding certification, the NIS2 framework is a European directive that has not yet been fully transposed into national law, which explains the current ambiguity around certification terminology.

From the floor

I would like to return to the issue of communication and behavioural responses. In your example of gas supply, did the public clearly understand the thresholds or trigger points that would lead to specific regulatory measures? In other contexts, such as water management or public health, populations are often aware of clearly defined thresholds—such as dam levels or vaccination rates—that trigger

behavioural restrictions. Did a similar system exist for gas storage levels, and did this influence your communication strategy?

Annegret Groebel | Bundesnetzagentur

During the crisis, we maintained a public dashboard displaying key indicators such as prices and storage levels, updated daily and often reported in the media. However, raw data alone is not sufficient; it must be accompanied by clear explanations. At the European level, we operate with a "traffic light" system, where different alert levels—green, yellow, orange, and red—are triggered based on predefined criteria, such as storage levels. Each level is associated with progressively stricter measures, including energy-saving recommendations or restrictions. Communicating these measures proved challenging. For example, when we suggested limiting non-essential energy use—such as heating private swimming pools—we encountered public resistance and negative media reactions. This illustrated that not all segments of the population fully grasped the urgency of the situation.

At the same time, communication had to be carefully balanced. We aimed to encourage responsible behaviour without creating unnecessary panic. For households, this meant promoting energy-saving practices, while for local authorities, it involved measures such as reducing public lighting. These actions had to be clearly framed as temporary and proportionate.

We also engaged in targeted communication with industry stakeholders, including energy producers and grid operators. During the peak of the crisis, daily coordination meetings were held—often early in the morning—to assess the situation, monitor indicators, and determine whether escalation thresholds had been reached. This allowed stakeholders to implement short-term mitigation measures proactively.

An important lesson from this experience was the value of professional crisis communication. We engaged a specialist to help refine our messaging, ensuring that it was clear, accessible, and effective. This was essential, as regulatory communication is not always easily understood by the general public.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

This highlights that in times of crisis, regulatory frameworks must evolve. The focus shifts from maintaining market efficiency to coordinating stakeholders and managing collective responses.

Davide Stroppa | EBA

In the financial sector, there is also a strong emphasis on proactive supervision. Regulators aim not only to respond to crises but to anticipate potential risks and intervene early. Communication is particularly sensitive in this context. For example, the results of stress tests must be carefully managed, as they can influence market behaviour. The EBA releases such information when markets are closed to avoid unintended consequences.

Arnaud Dietrich | CRE

We experienced similar coordination mechanisms in France during the 2022 gas crisis, compounded by challenges in the nuclear energy sector. During critical periods, daily coordination meetings were held between operators, producers, grid managers, government authorities, and the regulator.

One of the regulator's key contributions was the ability to aggregate and analyse data across the entire system, enabling informed decision-making. This demonstrates that pre-existing data capabilities are essential. The ability to collect and process data before a crisis occurs is a prerequisite for effective crisis management.

Eric Brousseau | Scientific Director, Governance and Regulation Chair

I would like to highlight an additional dimension related to the Digital Services Act. Given the complexity of digital platforms and the limited analytical capacity of regulators, the Act introduces an innovative

mechanism: it requires platforms not only to share data with regulators but also with the research community.

Researchers, subject to approval and safeguards, can analyse platform data to better understand systemic risks. This approach helps address the shortage of analytical capacity within regulatory bodies and leverages external expertise. While issues such as privacy and commercial confidentiality remain important, new techniques—such as synthetic data generation—can help mitigate these concerns. This model represents a complementary approach to regulation and may be applicable in other sectors facing similar challenges.

Closing Remarks

France Pégeot | Chair, OECD Network of Economic Regulators

Today's discussions highlight the evolving role of regulators. Beyond their traditional functions, regulators are increasingly becoming data collectors, analysts, and communicators. This transformation brings significant benefits—not only for regulatory effectiveness but also for society as a whole—but it also introduces new challenges and costs.

One key takeaway is that data alone is not sufficient. The value of data depends on the institutional capacity to analyse it and translate it into actionable insights. Another important aspect is transparency. Sharing data and analysis can improve compliance among regulated entities and empower citizens, thereby enhancing overall system performance.

At the same time, building these capabilities requires sustained effort, investment, and strategic focus. As demonstrated in several presentations, developing robust data systems and analytical capacities can take years and significant resources.

In this context, forums such as this seminar are essential. They allow regulators to exchange experiences, share lessons learned, and collectively address common challenges. The topic of data and digitalisation will undoubtedly remain central to our work, and we look forward to continuing this dialogue in future sessions.

A final point I would like to emphasise concerns the time and effort required to build effective data capabilities. This is often underestimated by those outside regulatory institutions. Developing systems that can properly collect, process, and protect data—while ensuring privacy and security—requires significant investment and time.

There is also a widespread misconception regarding the role of artificial intelligence. While AI offers valuable opportunities, it is not a "magical solution" that can instantly resolve complex problems. For example, in my role at the Canadian Transportation Agency, we handle a large volume of air passenger complaints. While AI is frequently suggested as a solution, its implementation requires careful design, integration, and oversight. Effective digital transformation cannot be achieved simply by adopting new technologies without the necessary institutional foundations.

A central theme of our work at the OECD Network of Economic Regulators is resilience. Much of what we do as regulators—whether through investment requirements, oversight, or service provision—aims to strengthen the resilience of the sectors we regulate. Today's discussions have clearly shown that data and digitalisation play a key role in this process.

Importantly, resilience is not only a characteristic of the regulated sector; it also depends on the capacity of the regulator itself. By developing robust data capabilities and improving operational effectiveness, regulators directly contribute to the resilience of the systems they oversee. This is a critical insight that emerged from today's exchanges.

Looking ahead, this topic will remain a priority for the OECD Network of Economic Regulators. As outgoing Chair, I am confident that my successor, Annegret Groebel, will continue to advance this agenda. The discussions we have had today—and the broader programme of activities—will contribute to ongoing learning and innovation in this area.

In conclusion, the sharing of experiences in an open and candid manner is essential. It allows us to learn from one another and to collectively address the challenges associated with digital transformation. This is an area that will continue to shape both the sectors we regulate and our role as regulators.

Chaire Gouvernance et Régulation
Fondation Paris-Dauphine
Place du Maréchal de Lattre de Tassigny - 75016 Paris (France)
https://chairgovreg.fondation-dauphine.fr/