A(I)FM – AFM and AI

Keynote Optic, October 2, 2024

By: Laura van Geest, Chair of the Executive Board at AFM

Ladies and gentlemen,

Here I am. A regulator among members of the financial sector. An EU citizen in a country of Brexiteers. My first association: Daniel in the lion's den. The Biblical story of Daniel taking a huge risk by going into the lion's den just because he remained true to his faith.

- But perhaps this association is too far-fetched. AFME is still a truly European organization.
- Supervisors and business do not have to be on opposing sides, on the contrary. We need to work together to keep the world a safe place.
- Relations between the UK and the EU may brighten up, under the new government.

I will escape. No divine intervention needed. Common sense alone will do the trick.

And this will be the theme of my talk. Collaboration to deal with the challenges that digitization brings. The challenges in the world of IT, the challenges in the world of AI.

On the political front, the UK and the EU may be separated, when it comes to our field of expertise – finance - , we are still very much connected. We are in the same boat, confront the same challenges and need to collaborate in order to tackle them.

If you were to see the financial sector as one big computer - a fitting comparison at this conference - we are connected just like circuit boards in one of the large financial servers.

And in this financial server, we depend on each other. Problems with a printer board in one any country, always finds its way elsewhere.

- Sparks in Germany, the Netherlands feels a sting
- Sparks in the Netherlands, England flares up
- Sparks in the chips of England, France feels a twinge. Or the Netherlands. Or Germany.

You get the idea.

We in the EU, including the UK, have a lot in common in a geopolitical sense.

- We both face the US from the west with all "the good, the bad and the ugly" associated with a Big tech that is developing into huge financial and data institutions, associated with Reddit forums that influence the global capital markets.
- We both face Russia, North Korea and China, from the east, confronting us with different questions and issues. Financial sector related, and beyond.

For us, it is crystal clear. We really need each other to keep financial markets safe.

Let me illustrate this with two examples from the IT world.

1. The risk of cybercrime. With increasing digitalization and the growing amount of sensitive data, banks, insurers, and other financial institutions are increasingly becoming targets of cyber-attacks, both from criminals and so-called stately actors.

   Financial institutions process huge amounts of sensitive information every day - personal customer data, financial transactions. This data is not only of great importance to the institutions themselves, but also popular booty for cybercriminals and interesting information for stately actors. Therefore, it is crucial that this data is well protected.

   As a supervisor, we see that with the arrival of DORA, there is more attention for the dangers of cybercrime and the importance of supervision of ICT risks.
   We believe it is important that institutions not only meet the requirements, but also understand how this helps them in controlling their ICT vulnerabilities. Preventing cybercrime is not something you do to please the regulator, it is in your own business interest!
   And with DORA, there will be a level playing field in the EU, as the same standard is used throughout Europe (EU).

   Many UK firms—especially smaller third-party ICT suppliers—may think they're in the clear, not being subject to these new requirements for cyber risk management and operational resilience. But that assumption is obviously wrong. The risks are real, they don't go away, just because you look the other way. And If I'm not mistaken the UK-authorities are also working on a new operational resilience framework that will hopefully differ not too much from those in DORA. As an advocate of IT security and a level playing field, I can only applaud this.

2. The risk of cloud concentration. In the financial sector, the hybrid multicloud is becoming the thing – and this comes with risks attached, 'cloud concentration' being the biggest risk.

   Multicloud means that business-critical functionalities of multiple financial institutions are invested in one cloud provider. A disruption at such a provider will therefore affect all these institutions, which can cause significant damage and even stability risks.

   Thanks to DORA, regulators gain more insight into the concentration of cloud services. The register of information helps us to map all third parties to whom ICT services are outsourced. In addition, it helps us to identify the critical third-party providers (CTPP) where the greatest concentration risks occur. DORA offers parties as ESMA, EBA and EIOPA the opportunity to monitor these critical service providers. For these critical service providers (and therefore also the cloud service providers) it is important that sufficient measures are taken to guarantee the availability, integrity and confidentiality of their ICT systems.

Let me recap . We become more and more IT savy and IT dependent. This increases the importance of Cybersecurity and Operational resilience as a precondition for business

survival. DORA is not something for IT nerds, it deserves full attention at C-level, both in business and among supervisors. And in the present unstable geopolitical environment, something that is best addressed in collaboration.

- Business and supervisors.
- ESA's and NCAs,
- EU and UK.

AI

Let me now turn to AI – the new kid on the block.

AI brings benefits to businesses and to the customer, but also risks. For the customer, for business and for the financial system at large.

At AFM, we have been delving into these themes for some time now. The print board 'Netherlands' indeed. Useful, but obviously far more effective if we work together. That is why it is great to talk about this topic here today. Remember the printer board, remember the sparks that can affect you as well.

Let me start off with some facts. In a study we conducted in 2022 focusing on major proprietary trading firms established in the Netherlands, we found that 80% to 100% of their trading algorithms rely on machine learning models.

The Machine Learning models used by prop traders continuously predict the future price of the financial instrument, based on which orders are changed or cancelled. The complexity of these models creates serious risks. Like the lack of explainability (the well-known black box phenomenon) and the possibility of manipulation.

Now, we expect companies to be able to explain why orders have been sent to the market. In addition, it is important that good first and second line controls are in place to prevent disruptions. This is especially relevant, as the focus of algorithms on the order book makes these algorithms sensitive to possible (intentional) disruptions in this order book, including manipulation.

After this primer, let's dive deeper in the world of AI;

- Collusion in algorithmic trading
- Modelling of the behaviour of trading algorithms using our data

Let's start with collusion algorithmic trading

At the AFM we did a deep dive into "collusion" between self-learning trading algorithms. But what are we talking about?

Some algorithms are self-learning: they can learn from their own behavior, so that they can figure out for themselves what the best action is in any given situation. This makes them better and better.

If these algorithms work together, they can arrive at their most advantageous action together: for example, the highest possible joint profit. Advantageous indeed, for them at least. We call this algorithmic collusion. This form of market coordination is potentially harmful (to put it gently).

Algorithmic collusion is more likely when markets are concentrated, transparency is high and interaction frequent. Sounds familiar? And it is a fact that trading on many capital markets is often dominated by a few players who account for the largest part of the trading.

Unfortunately, the current legal framework makes it near impossible to counter risks such as algorithmic collusion. Never mind how harmful. It is important that all parties involved take their responsibility so that together we ensure that the market continues to function well. This requires, among other things, a higher awareness of market parties and a willingness to face facts.

Of course, we are not just waiting for the market to come up with solutions that protect the financial sector. As a supervisor, we also take up this challenge. And are investigating the use of AI in trading algorithms to detect new forms of market disruption or manipulation.

This brings me to the second AI subject of today:

Modelling of the behaviour of trading algorithms using our data

In order to do our job as well as possible, we build statistical models that describe how market participants or “algorithms” choose the direction, price, and volume of orders.

Data is the magic word here. Collecting data, reading data, interpreting data. All in an attempt to guarantee ethical trading behavior, and robust and transparent markets.

Inspired by the well known Every breath you take song by the Police:

Every trade you make,
And every move you make
Every bond you break
Every step you take
I'll be watching you

My point: we see everything you are doing. Business-wise 😊. And that’s thanks to data and analyses.

It is a matter of rewinding the movie. And by rewinding the movie we hope to find the connection between the action the algo takes and the event that caused the action to happen at that moment.

An almost full automated process. Eventually a heatmap is formed from which we can read how the algorithms have done their work.

So this heatmap shows all the actions that the algo takes and what happened in the market before that. So we see what sets the algo in motion or what the algo responds to.

Such heatmaps are the new gold for supervisors. We gain insights into which algorithms are triggered by which event.

These analyses also allow us to find different groups of trading algorithms on the financial markets. Some are real “market makers”, while others might be more directional in nature. Displaying actions that might be harmful to the proper functioning of the markets.

And in this way we can also remove the black sheep - or perhaps more - from the herd, and it allows us to tackle manipulation.

Data-driven supervision at its best.

This is not a solo enterprise on the part of the AFM. We are developing this in close cooperation with the University of Oxford. As such, another excellent example of working together, between the Netherlands and the UK, between supervisors and academia, between the AFM and the FCA. Even in ‘AI world’, in-person contact is important. High tech, high touch.

Ladies and gentlemen,

Today I have taken you into a small part of the AI – maze, in a subset of the capital markets.

From a supervisory perspective it is exciting to walk through this maze. And I think my European colleagues see it this way as well.

As regulators we tend to think in terms of risks, tend to look at the glass half empty. Data quality, discrimination and exclusion, data protection, explainability and incorrect results.

And I also see that AI can bring opportunities.

AI can help with fraud prevention and detection, anti-money laundering and countering the financing of terrorism and cybercrime, credit assessments and identity verification. And that all sounds like music to my ears.

And with its computing power, AI can perform complex risk analyses using historical data and predictive models, helping financial institutions make informed decisions and minimize their risk exposure.

By sharing best practices, for example on occasions like this, we can understand each other better. You see the depth of individual AI developments, we see the breadth because we see the entire playing field. By working together and sharing knowledge, we can create a future in which AI is integrated into the financial world in a responsible and sustainable way.

This also requires interdisciplinary collaboration, collaboration with ethicists, lawyers, economists, and other experts. No one wants to discriminate, but things can go wrong with the technology. We are not omniscient, as financial experts.

And don't forget to inform society at large. By informing them about the benefits and risks of AI in the financial sector, we can help to promote a better understanding and acceptance of this technology.

As a sector, I would keep in mind, that we are not each other’s enemies during this process of AI innovation.

In fact, If I were you, I would embrace our supervision. Because citizens indicate that they have more confidence in AI when there is supervision. Does all this call for legislation additional to the AI Act? No, not necessarily. The standards that financial companies must comply with are, so to speak, largely 'technology-independent'. Even if we need some finetuning.

You already have a certain duty of care. And I assume that you already know what we expect from you.

Ladies and Gentlemen,

The world is changing in a world of bits and bytes, of IT and AI. It is new, exciting and challenging at the same time.

Both for business and regulators.

Let common sense prevail and work together. Especially in view of the geopolitical tensions.

That way we can move forward together and harness the potential that digitalization offers.

Thank you for your attention