Hedge Fund Law Report
An Acuris company

HFLR.com

May 14, 2020

TECHNOLOGY

The Current State and Future of AI Regulation

By Vincent Pitaro, *Hedge Fund Law Report*

Private fund managers are increasingly incorporating artificial intelligence (AI) into their investment processes. AI models, which incorporate vast amounts of data and may be hard to understand, present unique regulatory risks. Legal and reputational consequences of improper handling of AI should be avoided by fund managers.

A recent Debevoise & Plimpton program addressed the current state of AI regulation, AI governance, mitigation of risks associated with the use of AI and where AI regulation may be headed. The program also examined the potential use of AI in combating the coronavirus pandemic and the associated risks.

The webinar featured Debevoise partner Avi Gesser and associate Anna R. Gressel, as well as Matthew Homer, Executive Deputy Superintendent of the Research and Innovation Division of the New York State Department of Financial Services (DFS). This article synthesizes the panelists' commentary most relevant to hedge fund managers.

See "EY 2019 Survey Explores Growing Importance of Talent Management, Diversity and Inclusion; Use of Technology, Big Data and AI; and Cybersecurity (Part Two of Two)" (Dec. 19, 2019); and "AI for Fund Managers: How to Use It to Streamline Operations (Part One of Three)" (Sep. 5, 2019).

Trends in AI Regulation and Enforcement

In 2018 and early 2019, the question was whether there would be any AI regulation. In the past year, the conversation has shifted to when and how regulation will come, Gressel said. Not every regulator will come down with AI regulations, but there are some who are already articulating a more concrete regulatory framework.

Global View: Risk-Based Regulatory Approaches to AI

Present efforts to regulate AI are reminiscent of regulatory efforts with respect to cybersecurity a decade ago, Gesser noted, adding that regulators recognize an issue but are not yet sure how to regulate it. They may start by using an existing legal regime; develop new laws and rules based on general principles; and, eventually, adopt more precise rules. Regulators are using risk-based approaches to help prioritize their efforts.

Europe and AI Regulation

The European Commission (EC) recently released a white paper articulating its approach to AI regulation and is seeking comments on a proposed framework, which may incorporate existing liability frameworks while addressing new risks. For now, the EC is considering a

"risk-adjusted" approach to regulation, under which the higher the perceived risk of a sector, the tighter the regulation. A critical concern is how the EC will define "high risk." Further work on this undertaking that was originally expected for later this year may be delayed by the coronavirus pandemic.

At the same time, there are noteworthy legal cases regarding AI in the EC. For example, a recent case in Holland involving an automated system for detecting welfare fraud was notable because the judge applied human rights law to AI, Gressel said. The system was deemed by a district court in the Hague to violate Article 8 of the European Convention on Human Rights, which addresses the right to respect for private and family life, home and correspondence. "I think that was a surprising result for observers in this area because of the application of human rights law to AI," commented Gressel.

In contrast, AI cases in the U.S. have been focused on due process violations.

New York Perspective

The Research and Innovation Division of the DFS is focused on supporting responsible innovation like AI, which offers huge potential benefits but also poses big risks in the markets, Homer said. The Research and Innovation Division identified four overarching areas of concern:

1. What data is fed into the model? Is it needed for the decision at hand or is it a proxy for something else?
2. Is the model understandable and transparent? How was it developed?
3. Are the model's outputs fair and nondiscriminatory?
4. What is the effect of the process on consumers and the general public? Do they understand the results? Are they able to act on the results?

For discussion of regulators' use of AI, see "Former OCIE Director Carlo di Florio Discusses the SEC's National Exam Program, Technology and CCOs (Part Two of Two)" (Nov. 21, 2019).

AI Governance Mechanisms

Another regulatory concern, especially in the E.U., Singapore and Hong Kong, is having sufficient governance over AI and appropriate reporting lines, Gressel added. Some regulators are focusing on appeal rights, including the ability to obtain an explanation for an AI decision; ways to potentially change the decision; and the ability to speak with a human being and, possibly, to have someone else take a look at the decision, Gesser said.

Even in the absence of definitive regulation, businesses have been thinking about adopting appropriate governance for AI models, Gesser observed. When considering governance, Homer explained, businesses should think about the four overarching regulatory concerns listed previously and expect questions from regulators, including:

- What is the model being used for? For example, is it for a consumer-related decision or fraud monitoring?
- Where is the greatest risk of harm to consumers?
- What data is included; is it correlated with protected class data; and is it relevant to the product or service in question?
- How is the model being developed and trained? Is the model trained by a machine or a human?

- Can the model be explained?
- How is the model overseen; tested for bias and unfairness; and refined?
- Are model outputs being reviewed and analyzed? If so, what actions are taken when disparities occur among outputs?
- Are consumers receiving sufficient and transparent information about the model and the decisions being made, and do they have recourse if they are dissatisfied with a decision?

A firm should have an internal structure to support AI governance, just as it would for other products, Homer added. Policies and procedures should support responsible use of AI tools. In addition to technical specialists, there should be input from legal and compliance to identify, mitigate and monitor risks. Lawyers and compliance personnel can help think about how regulators might approach an issue and to what they will respond.

Lawyers can contribute meaningfully, even if they lack technical expertise, Gesser opined. It may not be possible to have someone on staff with sufficient AI expertise, Homer said. What is important is knowing what questions to ask, speaking to experts and conducting careful due diligence.

AI is becoming more closely intertwined with core business functions, Gressel noted. The level of knowledge needed will depend on the industry. Regulators are focusing on what people do not know and cannot explain. Therefore, it may be necessary to get into the weeds to figure out what can be known about a given AI system and its limitations. Lawyers, who usually focus on causation, will have to grapple with the fact that AI is predictive and deals with correlation and statistical levels of confidence.

For discussion of the use of AI in regulatory reporting and compliance, see "FINRA RegTech Conference Reviews AI, RegTech Adoption and Compliance Challenges (Part Two of Two)" (May 30, 2019); and "FINRA RegTech Conference Examines AI and Big Data; Blockchain; and Regulators' Views (Part One of Two)" (Mar. 21, 2019).

Applicability of DFS Life Insurer Position

Homer noted that in a January 2019 circular letter to life insurance companies, the DFS outlined three main points related to those insurers' use of alternative data sources:

1. An insurer should not use alternative data sources unless it can show that the data has a strong actuarial basis and does not use prohibited criteria.
2. Ultimate responsibility for AI models lies with supervised insurers, not their vendors.
3. Consumers must receive sufficient information about what data was used when declining coverage.

Those themes could apply to other financial services firms, especially for ensuring fair and nondiscriminatory outcomes, Homer observed. The DFS continues to work on that issue and is engaging with experts and other regulators. It is taking a risk-based approach for the time being.

The letter also illustrates how regulatory concerns develop as a new technology such as AI evolves, Gesser noted. Data scientists will have a very broad view of what data is relevant to AI models. On the other hand, not all of that data will pass legal muster.

For more on the DFS, see "Proposed Expansion of New York Department of Financial Services Could Impact Hedge Funds" (Apr. 16, 2020).

Risk Reduction Strategies

While the regulatory framework is under development, it is important for fund managers to reduce their risk when using AI. For now, it may not be possible to tell a manager precisely what it should do, but it is possible to see if a manager is trying to do the right thing, Gesser observed.

Managers are thinking about how to test for regulatory or reputational risk in AI models, Gressel added. Key concerns include monitoring models, many of which are adaptive and change constantly; answering questions about the models; and deciding when to involve a human being.

Repurposing Data for AI

According to Gesser, managers repurposing existing data for use in AI applications should consider whether:

- repurposing data is consistent with existing contractual or privacy obligations;
- moving data from one application to another increases cyber risk;
- a new use of data is riskier than the original use for which it was collected; and
- a change of use is consistent with applicable policies and procedures.

A manager should make sure it has the right to use the data for the new purpose. When repurposing data, it needs to ensure the new use is consistent with all contractual and privacy obligations. It also need to secure the old and new data. Also, every time data is repurposed, the manager needs to go through its policies and procedures and confirm that the new use is appropriate.

See "AI for Fund Managers: Automating the Legal Department and Maintaining Privacy (Part Three of Three)" (Sep. 19, 2019); and our three-part series on the opportunities and risks presented by big data: "Acquisition and Proper Use" (Jan. 11, 2018); "MNPI, Web Scraping and Data Quality" (Jan. 18, 2018); and "Privacy Concerns, Third Parties and Drones" (Jan. 25, 2018).

Vendor Risk

A substantial amount of AI functionality will be provided by vendors, Homer said. Nevertheless, a manager is responsible for all of its actions, regardless of whether it outsources AI to a vendor, Gesser cautioned. Managers must employ their usual vendor risk management processes and engage with their AI vendors to ensure that they understand, and can justify, what their vendors are doing. The fact that AI is an emerging technology, coupled with the potential for consumer harm, means that managers should be exercising especially careful oversight of AI vendors.

Vendor management is an extremely important concern, Gressel stressed. A contract with an AI vendor should include provisions for appropriate controls and oversight and specify the vendor's obligations in case the manager is the subject of a lawsuit or regulatory action.

Contractual representations and cooperation duties are necessary but not sufficient, Gesser added. A manager that uses an AI vendor must conduct careful due diligence and implement appropriate controls. It must be able to show that it is being responsible for the AI that it uses.

See "AI for Fund Managers: Government Guidance, Service-Provider Negotiations and Risks of Bias (Part Two of Three)" (Sep. 12, 2019); "How Fund Managers Can Develop an Effective Third-Party Management Program" (Sep. 21, 2017); and "Key Considerations for Fund Managers When Selecting and Negotiating With a Cloud Service Provider" (Sep. 21, 2017).

Documentation

Documentation of AI use is also critical, Gesser emphasized. Many managers are approaching AI carefully and seriously, but they are not keeping track of their efforts. In the event of regulatory inquiry or media scrutiny, those managers may be unable to show what they have done. Therefore, as part of their AI governance, managers should keep contemporaneous records of their deliberations and actions.

Intellectual Property

Firms that use AI should consider whether the AI models include protectable intellectual property, Gesser advised. Similarly, they should consider whether use of the model's data inputs violates a third party's intellectual property rights. That is more of a business risk than a regulatory one, he added.

See "How Can Hedge Fund Managers Prevent Theft of Proprietary Trading Technology and Other Intellectual Property?" (Aug. 19, 2009).

Using AI to Track Coronavirus Infections

AI has been in the news recently, particularly as a tool to fight the coronavirus. For example, contact tracing apps that use AI can be used to identify people who are at high risk of having been in contact with a person exposed to the coronavirus, Gesser explained. If millions of people use those apps, AI will be essential for processing the information they gather and judging who is at risk.

The models may rely on Bluetooth, GPS, downloaded apps, existing apps or the operating system, Gesser continued. The data that goes into the models also varies. Some apps alert a user who has had contact with an infected person and requires that user to isolate him- or herself. Others permit the user to record symptoms. Still others impose travel restrictions based on risk profiles. As to what data is needed by those apps, some use age and health history to determine the risk of needing hospitalization.

China, Taiwan, South Korea, Hong Kong and Singapore all have had some success with using those apps to permit people to go back to work, Gesser noted. The U.S. and the E.U. have been looking into which of the many available models might be suitable for them.

The apps, however, give rise to significant privacy and security concerns, as well as the risks of both false positives and false negatives. In the coming weeks, public health authorities will have to balance the potential benefits of tracking apps with privacy and cybersecurity concerns and, in the U.S., Fourth Amendment and due process concerns. Key issues include:

- what data will be collected and how;
- who will have access to the data;
- how the data will be used;
- whether widespread adoption – which is critical to a program's effectiveness – is achievable; and

- whether the program should be voluntary or mandatory.

AI will be a large part of that analysis for coronavirus and contact tracing, and the pandemic will inevitably make AI even more important.

For more on the coronavirus pandemic, see "Key Considerations for Private Fund Investors Navigating the Coronavirus Crisis" (Apr. 23, 2020); and our three-part series on how fund managers can withstand the pandemic: "Form ADV Filing Relief, Investor Communications and Fund Valuation Issues" (Apr. 2, 2020), "Marketing Disruptions, Key Person Clauses and Cybersecurity Concerns" (Apr. 9, 2020), and "Business Continuity and Other Operational Risks" (Apr. 16, 2020).

The Future of AI Regulation

Regulators are thinking about broad principles applicable to AI, including the need for transparency, governance, testing and controlling for bias, Gesser said. Regulations fall on a spectrum from principles-based to highly prescriptive, Homer explained, and for each issue, regulators need to decide where it falls on that spectrum. For example, as the use of social media grew, the DFS decided that new regulations were not needed. Instead, it issued guidance as to how existing regulations applied to social media.

A principles-based approach to AI seems to make sense for the time being. There have been calls for additional guidance on AI, but it is not yet clear what that guidance should look like, he noted. The DFS would like to hear the concerns of industry and other stakeholders.

For the time being, it appears more likely that businesses that use AI will get into trouble for violating principles of existing regulations, rather than any AI-specific regulations, Gesser said. For example, a lender that uses a biased AI model for underwriting could run afoul of anti-discrimination laws. It would be helpful for regulators to provide examples of where that could happen. In addition to bias, regulators may also focus on the robustness of AI models; their security, verifiability and evidence of soundness; and testing, Gressel added.

For many managers, reputational risk is a bigger concern than regulatory risk, Gesser noted. It is important to think about how to promote public confidence and trust in AI tools, Homer said. Regulatory compliance may not be sufficient to do that. Organizations that use AI should think about additional ways to build trust.

See also "The Death of Alpha: A True Challenge or a Poor Manager's Excuse? DMS Summit Discusses Alpha Generation, '2 and 20' Fees, AI and Impact Investing" (Apr. 12, 2018).