Artificial Intelligence and Cybersecurity in M&A – A Swedish perspective

By Carl-Olof Bouveng and Yousef Chakir

How is AI affecting M&A practice?

Current use of AI

In Sweden, artificial intelligence ("**AI**") is widely discussed, tested and evaluated. While law firms have a long-standing history of using technology to leverage their M&A practices, recent developments within the AI research field have opened new opportunities for law firms to optimize their work and minimize transaction costs and time. The services and products, which commonly use various machine learning algorithms, aims at identifying issues in contracts during the due diligence phase. There are many providers which are keen to reach the Swedish market and engage in cooperation with law firms and others to test their platforms.

While the use of AI in generation of corporate documentation (general meeting minutes, board meeting minutes etc.), eDiscovery and similar tasks has reached prevalence, the use of machine learning to leverage due diligence reviews or generation of core transaction documentation has not yet achieved traction. However, after having evaluated several machine learning services, our view has been that current AI software has not yet reached sufficient maturity and integrability to replace traditional and manual labor of attorneys conducting the due diligence reviews. Nevertheless, it may be used as a mean to supplement the manual labor, for example for review of agreements that have been considered less material and which without AI would have been exclude from any kind of review.

AI in five years

We know that AI products and services have the potential to lower transaction costs, accelerate time to closing and increase the scope of reviewed documents due to efficiency advantages. As such, while the technical maturity of the services and products offered on the Swedish market improve, we assume that the use of AI software in the transaction process will increase within the next five years.

AI software is also likely to become an increasingly valuable tool in preparing transaction agreements and in particular to ensure that warranties and indemnities are tailored to the material reviewed and the findings in such review. For example, if the due diligence material contains documentation relating to real property also the warranties should cover such properties and if there are change of control clauses there should be warranties or indemnities covering the risks relating to such clauses. By the application of AI this process could be automated.

It can also be expected that law firms will approach new technology such as AI in different ways. Leaving aside firms that entirely neglect the development and stay passive, firms more actively developing a strategy taking into account new technologies may do so in various ways. Some firms, and not least the larger firms, may choose to develop software in-house or in a closely integrated "incubator", and actually employ personnel to develop and tailor software to the legal practice. Others may enter into cooperation with software developers to ensure that the technology is tailored to legal practice while the law firm and its personnel may continue to focus on legal services. Obviously, bar rules on ethics will play a role in how far any in-house arrangement or cooperation can be taken.

Managing AI risks

The use of AI software brings new challenges in terms of liability, the most significant risk being, as regards due diligence reviews, the risk of missing relevant clauses in contractual agreements. While the process of identifying problematic clauses in agreements will improve over time, certain issues are likely to stick around as machine learning software is self-contained to its input. A clause can be problematic in and of itself – which allows for generalization - or it can be problematic due to the context it exists in. For instance, a machine learning software will have a tough time determining whether two parties operate in the same market, which may be relevant in assessing a clause, although it can flag the clause for review irrespective of the parties' positions on the market.

In implementing AI/machine learning in due diligence reviews, law firms will have to assess the inherent risk in using such software and mitigate risks accordingly. Some risks will be mitigated primarily through careful diligence when selecting an AI vendor and some will be mitigated by soft means, such as user education. While an AI software may eliminate risks of missing clauses which it has been trained to find, the risk of human errors (such as incorrect handing of the software or flawed design) will likely not be eliminated completely. As risk cannot be eliminated completely, law firms will be obligated to inform clients of residual risks.

In cases of mistakes caused by AI software or incorrect use of AI software, it is currently unclear what the legal allocation of risk is between the law firm conducting the due diligence, the supplier of the AI/machine learning software and the client,. Largely this may be provided for in the terms of engagement, but we have not yet on the Swedish market seen any more sophisticated or novel approach to allocation of risk when AI is used in M&A.

The risk may also be covered by insurance but it will then take some time before the market will feel comfortable about the insurance underwriters picking up the tab. In M&A we have previously seen how insurance over the years have taken an increased share of the risk under representations and warranties but only after the market having got comfortable with the insurance underwriters actually having honored claims under such insurance policies.

AI in acquisition targets - Due diligence, and representations and warranties?

While AI software has yet to become prevalent in M&A practices in Swedish law firms, in terms of software that performs non-basic tasks, it is becoming increasingly common for

acquisition targets to leverage AI as businesses reorient towards a more data-centric business model.

There is no ownership of data in the traditional sense as the ownership of data is rather negatively defined - an acquisition target may use data unless there are contractual or regulatory encumbrances (i.e. provisions on intellectual property rights, personal data, trade secrets or anti-trust laws). This multi-facetted "ownership" of data may lead to data assets having to be reviewed by lawyers with different perspectives in order to identify all relevant legal issues.

The following table illustrates at a high level the relevant issues that may be covered in a due diligence review.

Operation	**Contractual**	**Legislative/Regulatory**
Data in (transfer)	License in terms (IP) Supplier availability	Transfer restrictions • Privacy/GDPR • Anti-trust laws
Processing operations	License in terms (IP) Other contractual limitations • Non-compete • NDA	Processing limitations • Privacy/GDPR • Sector specific legislation Security requirements • Privacy/GDPR • NIS • Sector specific legislation
Data out (transfer)	License in terms (IP) License out terms Confidentiality	Transfer restrictions • GDPR • Anti-trust laws

The regulatory landscape surrounding data is changing fast and the introduction of regulatory frameworks such as the General Data Protection Regulation ("**GDPR**"), the Directive on security of network and information systems ("**NIS Directive**") and local privacy laws does present certain challenges. While some regulatory provisions only introduce security requirements, consumer rights or prohibitions to use certain data assets, privacy law stresses the importance of why certain information is processed. This requires an understanding on an operational level of why certain data assets are processed when the data assets concern individuals.

Cybersecurity

General

Data is becoming increasingly important and valuable as acquisition targets reorient towards data driven business models. Any cybersecurity review should therefore seek to establish whether conditions exist to protect the data and preserve the value of such data, and the ability to use the data. This would include third party data but also the target's own data.

The general approach to cybersecurity is the same as for information in general – the goal being the protection of *confidentiality*, *integrity*, *availability* of data and information.

Cybersecurity review

A lot have changed with the onset of the GDPR and the NIS Directive and is likely to change again with the ePrivacy Regulation. Most privately-owned companies have historically not been subject to any regulatory information security regulations of substance, other than if the acquisition target's business was subject to sector specific legislation.

The information disclosed under a due diligence review is limited, as is the time under which the due diligence review is conducted. Cybersecurity reviews are therefore focused at establishing whether the acquisition target have adequate processes and policies for managing cyber security risks, such as if it has implemented any information security management systems (e.g. ISO 27001). This is in line with regulatory requirements placed upon acquisition target. Most of the regulatory frameworks doesn't prescribe certain security measures but rather a risk-based methodology. Besides more specific regulatory frameworks any review would need to consider the standard in the particular industry, and therefore detailed knowledge of the relevant business sector is important.

Contractual engagements, or the lack thereof, are reviewed within the scope of the cybersecurity review in order to establish, among other things, whether:

- employees, third parties or other recipients are subject to NDA:s
- the acquisition target has entered into adequate SLA:s with suppliers
- data processing agreements have been entered into with the acquisition target's processors.

Warrants and representations, and indemnities

Residual risks are handled in cyber-specific representations and warranties which generally covers past data breaches, conformity to regulatory requirements and to internal processes or policies.

In case breaches or other issues have arisen in the due diligence, it may be necessary for the buyer to seek an indemnity from the seller. Such indemnity should cover not only regulatory penalties and damages, but also the costs of taking remedial actions and put in place proper procedures. However, any reputational damages a company may suffer may be harder to cover.

The exposure and costs involved in a cybersecurity breach may be significant and it may be hard for the parties in a transaction to agree on a risk allocation and for either party to be willing to assume the risk. A solution in this context may in some cases be insurance. The premium may be high but possibly the only solution to avoid that the transaction stalls.

Prevalence of cybersecurity reviews

On the buy-side, cybersecurity review is not often specifically requested and the review is therefore usually performed at the level described in above. The review is then aimed at establishing whether the acquisition targets have methods and processes for managing information security issues and residual risks are covered in cybersecurity/regulatory reps and warranties Cybersecurity review may be specifically requested when the acquisition target operates in highly regulated areas (life science, banking, fintech).

We usually do not meet specific cybersecurity requests or requirements when representing the sell-side, nor have we encountered requests for obtaining cyber insurance policies. In summary, we would assess that cybersecurity is not a prioritized area by clients or generally among Swedish law firms.