Data ethics — why should you care?

Karishma Brahmbhatt, Senior Associate at Allen & Overy, explains why organisations should be focussing on their data ethics

The concept of data ethics, once confined to academic discourse, is increasingly infiltrating corporate corridors. This is not surprising, given data is one of the most valuable assets that organisations have at their disposal.

We live in a data-rich era. Data-generation has become an inevitable constant of life in our interconnected and technology-driven society. The widespread availability of sophisticated tools for measuring and deciphering immense data troves offers organisations the potential to unlock hidden insights into their customers and employees, identify and realise business efficiencies, and detect and predict market trends. From an organisational standpoint, data generation has ended up being as much intentional as it is incidental. The potentially limitless opportunities provided by data-driven insights have in recent years led to almost all organisations being data-focussed to some extent and, as such, acquiring a data-risk profile that needs careful management. This is where data ethics becomes relevant.

What is data ethics?

Data ethics is the study and evaluation of moral problems relating to data, algorithms and corresponding practices to formulate and support morally good solutions (Floridi L, Taddeo M. 2016 'What is Data Ethics' Phil.Trans. R. Soc 374:20160360). In practice, data ethics embodies the difference between what companies *can* do with data, and what they *should* do with data. Technologies such as artificial intelligence amplify and add new dimensions to ethical uses of data, but the concept of data ethics is technology-agnostic. This means that it is equally relevant to other data-rich activities undertaken by companies, such as social listening.

The boundaries of what is considered to be 'acceptable' data use are fluid and constantly shifting, which creates an uncertainty that has the potential to catch organisations off-guard. Thinking about data ethics in a corporate environment is certainly not easy, but ignoring it can significantly affect an organisation's reputation and commercial operations. Put simply, data ethics is one of the most operationally complex risk management challenges facing organisations today.

Why should you care about it?

The philosophical roots and idealistic tendencies that the concept of data ethics may conjure makes it prone to dismissal by stakeholders as being too nebulous and theoretical to have any real application in the business world. Indeed, economist Milton Friedman famously argued that "there is one and only one social responsibility of business — to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game, which is to say, engages in open and free competition without deception or fraud" (Milton Friedman, Capitalism and Freedom (1962)).

So why should organisations invest resource in addressing data ethics?

1. Because regulators care, and are increasingly focusing on the issue

There are various laws across the world that seek to regulate the use and collection of data (particularly personal data). However, events over the past few years have shown a gradual shift to a socio-political environment in which, at least when it comes to data, arguing compliance with the letter of the law is simply not enough to win favour with regulators and consumers.

Instead, organisations also need to be able to show a commitment to the spirit of the law. This need for organisations to focus on the ethical dimension of data processing has been emphasised by regulators across the world, from the European Data Protection Supervisor, the Information Commissioner's Office in the UK and the CNIL in France, to the Federal Trade Commission in the United States and the Privacy Commissioner for Personal Data in Hong Kong. Some regulators have even expressly recommended that, as best-practice, organisations should sign up to "a set of ethical principles to build trust with… customers [and make these principles] … available on [the organisation's] website and on paper" (see the ICO's

Guide to the General Data Protection Regulation: Individual Rights, available on its website).

Since at least early 2018, regulators have implied a willingness to use legislation to penalise organisations for failure to process data in an ethical manner. The fact that data-focused legislation enshrines — expressly or implicitly — data ethics principles makes it easier for regulators to achieve this aim.

The EU General Data Protection Regulation ('GDPR') is a case in point. Several ethical principles most commonly championed by the growing body of data ethics guidance have been woven into the fabric of the GDPR; for example, the GDPR advocates data to be processed for societal good, entrenches principles of fairness and transparency of processing, and requires accountability for processing activities. (Recital 4 states that 'the processing of personal data should be designed to serve mankind'. For examples of fairness and transparency, see Recitals 39, 58 and 60, and Article 5(1)(a) and 12-14. For examples of how accountability is enshrined, see Recital 85, and Articles 5(2), 25 and 35, among others).

Since the GDPR was introduced, jurisdictions around the world, such as Brazil, Israel, Tunisia and Thailand have been updating their data protection laws to reflect GDPR-type concepts.

Ethical undertones help to make legislation dynamic, adaptable and relevant in an age of evolving technological innovation. They provide regulators with the agility to use otherwise rigid legislative provisions to address concerns over data monetisation in the context of innovative technologies and processing activities (such as artificial intelligence, adtech and facial recognition).

This intertwining of law and data ethics means that, in practice, regulators already have access to tools for penalising organisations for data processing behaviours perceived to be unethical.

As a consequence, organisations can no longer manage data risk as purely a box-ticking exercise. To reduce risk of regulatory action, and to be seen to be processing data in a way that is both legal and socially acceptable, organisations need to overlay their data compliance programmes with a values-based approach to data processing.

> ***"This intertwining of law and data ethics means that, in practice, regulators already have access to tools for penalising organisations for data processing behaviours perceived to be unethical. This means that organisations can no longer manage data risk as purely a box-ticking exercise."***

2. Because consumers also care, and are (sub)consciously engaging with the issue

The notions of data privacy, data use, and the way in which data can and should be used by those seeking to benefit from it, have been brewing in the public consciousness for a while, triggered by Edward Snowden's revelations about the activities of government intelligence agencies. A series of high-profile events exposing the way in which data are monetised (such as in the Schrems v Facebook cases and the Google Spain 'right to be forgotten' case), followed by the much-publicised implementation of the GDPR, has helped to raise awareness of individual rights when it comes to third party use of their data. This, together with the proliferation of social media, has given consumers some knowledge, and a public platform, for voicing their concerns.

Today, more than ever before, consumers have the power to dent an organisation's reputation, trust and — ultimately — profits, if they perceive data processing activities to be unethical; there are plenty of anecdotal examples of this. The consumer-led pressure on organisations to behave (and, perhaps more importantly, to be seen to be behaving) responsibly and ethically is supplemented by public campaigns by the likes of Privacy International, Brave and None of Your Business, which are just some of those seeking to hold organisations to account over their data processing activities.

So, what does this mean for organisations that are interested (or have invested) in processing data? It means that now, more than ever before, consumers are assuming the role of unofficial 'regulator' of organisations' data-related activities. Consumers are not afraid to comment on how they think organisations are and should be using data. At worst, their disparaging online comments may go viral, generate media interest, lead to consumer-boycott and trigger regulatory interest in the organisation's activities, thereby causing something of a PR nightmare for organisations and compounding the 'trust deficit' that regulators have perceived in modern business and innovation.

Proactive engagement with data ethics and establishing an ethical data culture can help organisations to defend their data processing activities. This is especially the case where there is a risk that their activities, although strictly legal, could be perceived as inappropriate, invasive and, ultimately, socially, morally and ethically questionable.

3. Because investors are investing in the issue

The increased regulatory and consumer interest in ethical data use, coupled with the significant value to

(Continued on page 8)

(Continued from page 7)

be derived from prudent and innovative uses of data, means that data ethics is relevant to both *value*-driven and *values*-driven investment. Particularly since the GDPR came into force, we have seen examples of investors reacting to perceived unethical uses of data by the companies in which they have invested. Businesses have seen their share prices dip (at least temporarily) in the aftermath of their data-related activities being considered to be unethical (for example, 'Over $119 billion wiped off Facebook's cap after growth shock', *The Guardian*, 26th July 2018), whilst investors in London's King's Cross development launched an investigation into the developer's use of facial recognition in the area ('King's Cross investor seeks facial recognition answers', *BBC news*, 19th August 2019).

Given the importance of data management to an organisation's business strategy, it is unsurprising that investors are more actively urging companies to remedy perceived ethical deficiencies in their data management practices, suggesting that it is only a matter of time before data ethics makes its way on to the environment, social and governance (usually referred to as 'ESG') agenda of organisations.

Conclusion

With the emergence of ethics as a focal point of regulatory dialogue and consumer activism, organisations cannot risk neglecting the ethical angle of their data-based activities. Establishing an appropriate internal approach to data ethics can help an organisation to manage its regulatory, reputational, and investment-related risks through setting the parameters of what is commercially achievable by reference to what is socially acceptable.

It is becoming ever-more apparent that, to keep up with evolving technology and customer demand, organisations are having to tread the line between business advancement on the one hand, and managing (and responding to) public perception and expectation on the other. Get it wrong, and their data management practices could be perceived as 'underhand' or 'creepy', potentially triggering public outcry and regulatory sanctions. Get it right, and privacy and ethics may well end up being the organisation's unique selling point.

Karishma Brahmbhatt
Allen & Overy
karishmabrahmbhatt@allenovery.com