Client Alert: Artificial intelligence and GDPR – teaching machines 'fairness'

Date : May 28, 2021

Introduction

This week the Chair of the European Parliament's committee on AI expressed concerns about the enforcement of the European Commission's proposed AI rules, which he said could create national fragmentation similar to that seen with the GDPR. So what are the issues involved, what is the proposed new EU law and how does GDPR already regulate AI?

Use of AI

At the start of 2020, 42% of companies in the EU said they use technologies that depend on AI, and another 18% of companies said they are planning to use AI in the future (European Enterprise Survey – FRA, 2020). So, this is clearly an area that is justifiably generating considerable activity and interest from both industry and the regulators.

It is important to note however that currently the available technologies involve varying levels of complexity, automation and human review and, despite some companies' optimism about their AI capabilities, many applications currently used remain in the development stage. We've also seem some technology billed as 'IA' be little more than basic code with a nice wrapper. For many as a result, AI is still on the journey from being an emerging technology to becoming fully embedded into companies' BAU systems. It follows that some of the regulation and guidance in this area is also still 'in development'.

Does data protection law apply to AI?

Usually yes. To the extent that personal data is processed using AI, the existing framework of data protection laws will apply. This can raise some interesting technical, legal and ethical challenges, in particular, where the outcomes produced by machines (like in humans) could be skewed by inherent biases. To that note, since we first published this alert in March 2021, the European Commission has released its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) on 26 April 2021 to address the risks of AI (see below).

In this article, we take a deep dive into AI and GDPR, including recent highlights that illustrate the current thinking from the European bodies and regulators on this complex issue. There are some technical terms in this note that are explained in our glossary at www.bit.ly/gdprwords.

Key technical concepts: AI, machine learning and deep learning

GDPR does not define AI and there is no universally accepted definition. However, the UK Government Office for Science in its paper 'Artificial intelligence: opportunities and implications for the future of decision making' (9 November 2016) defined AI in terms of its outcomes as:

"…the analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events."

The European Commission, in its 2018 Communication on Artificial Intelligence, used a broadly similar definition that has more emphasis on the 'intelligence' component:

"systems that display intelligent behaviour by analysing their environment and taking actions—with some degree of autonomy—to achieve specific goals."

The Commission went on to describe the application of AI:

"AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications). We are using AI on a daily basis, e.g. to translate languages, generate subtitles in videos or to block email spam. Many AI technologies require data to improve their performance. Once they perform well, they can help improve and automate decision making in the same domain."

"Machine learning" and "deep learning" go hand in hand with AI – in short, deep learning powers machine learning, which ultimately can enable AI.

Machine learning is a design methodology for AI. According to the European Parliament's study on 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (June 2020) ('EP Study'):

"Machine learning systems discover correlations between data and build corresponding models, which link possible inputs to presumably correct responses (predictions). In machine learning applications, AI systems learn to make predictions after being trained on vast sets of examples."

Deep learning is a method of machine learning, and may include deep neural networks (DNNs). Some common applications of deep learning include image recognition, voice-enabled software, and real-time translation apps.

Key legal provisions:

Various different parts of GDPR have an impact on the regulation of AI-driven technologies, including:

1. Article 5 – data protection principles, in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy and storage limitation / retention
2. Articles 6, 9 and 10 lawfulness of processing
3. Articles 12, 13 and 15 – transparency of processing
4. Article 22 – rights in respect of solely automated decision-making (and other data subject rights)
5. Article 25 – data protection by design and by default
6. Article 35 – data protection impact assessments (and prior consultation (Article 36))

It should also go without saying that AI systems need to ensure the data within them is kept secure (Article 32).

You will also need to consider if any other laws or local or sector-specific laws apply, depending on the context and purpose of the relevant technology and what it actually does.

Applying GDPR to AI

We have expanded below on some of the more substantive legal issues and challenges related to AI:

Transparency

Transparency essentially means giving people clear information about how their personal data is processed using AI and any potential impact this may have on their privacy. It must be obvious to people that their data is being collected and how it is being processed, including how decisions are being made about them. Processing is unlikely to be transparent – and may also not be fair and lawful – if personal data is used by AI systems in ways in which people would not expect.

An example of automated decision-making powered by AI that people may not necessarily be aware of, which was given in the UK ICO's guidance on 'Big data, artificial intelligence, machine learning and data protection' (2017) ('ICO AI guidance'), is the use of social-media data for credit scoring.

Transparency is usually achieved through providing a privacy notice to the individuals whose data you are processing. It is a key element in ensuring processing of personal data is 'fair' (see below) and in building trust with individuals.

There is also the issue of algorithmic transparency, which means that people are given information about how algorithms work and there are checks to ensure that these are working properly (e.g. audits – see ‘Algorithmic audits and governance measures’ below). If personal data is being processed by automated means GDPR gives data subjects additional rights – for example to know about this processing under GDPR Art. 14(2)(g) and the right to object to this form of processing in some circumstances under GDPR Art.21 & 22. In our experience there’s often a tension in this area. Providers of AI solutions often want to sell those solutions on a ‘black box’ basis and are often reluctant to be specific as to how they are using AI, the algorithm they are using and the criteria for any decision as they see that as the basis of their commercial success. Equally anyone procuring those services will usually want to know these details to consider the compliance impact of an AI solution and ensure that the organisation’s transparency obligations under GDPR can be met.

Data minimisation

Organisations need to minimise the amount of data they collect and process. This can prove a challenge when AI tends to work over massive datasets. The ICO’s AI guidance says:

“Organisations therefore need to be able to articulate at the outset why they need to collect and process particular datasets. They need to be clear about what they expect to learn or be able to do by processing that data, and thus satisfy themselves that the data is relevant and not excessive, in relation to that aim. The challenge is to define the purposes of the processing and establish what data will be relevant.”

Anonymisation and pseudonymisation also have an important part to play in reducing the amount of identifiable data that is collected and used. Anonymised data is not ‘personal data’ within the GDPR definition. However, pseudonymisation is a security technique only, meaning that pseudonymised data is still personal data and as such the GDPR rules still apply to it.

Fairness and bias

There are risks that algorithmic decisions may be mistaken or discriminatory. This is particularly the case where the outcome is based on using special category data features (predictors) such as race, ethnicity or gender. In addition, a system’s outcome may be discriminatory if it disproportionately affects some groups without a supportable reason.

The European Data Protection Supervisor (EDPS) in its ‘Opinion on the European Commission’s White Paper on Artificial Intelligence – A European approach to excellence and trust’ (2020) raised specific concerns about the risks associated with remote biometric identification, and:

“supports the idea of a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place and until the moment when the EU and Member States have all the appropriate safeguards, including a comprehensive legal framework in place to guarantee the proportionality of the respective technologies and systems for the specific use case.”

Also, the Dutch Government recently came under fire from commentators for its failure to address institutional racism where the tax authority had used discriminatory methods to identify alleged cases of fraud, which relied on singling out people for special attention because of their ethnic origin or dual nationality.

In fact, we have seen a broader trend in cases from the regulators focussing on ‘fairness’ issues. See for example, the following Cordery alerts involving CaixaBank (Spain), Notebooksbilliger (Germany), H&M (Germany) and Grindr (Norway).

Solely automated decision-making

Where AI is used in decision-making concerning individuals, again issues regarding fairness and discrimination arise. According to the EP Study:

"The alternative to automated decision-making is not perfect decisions but human decisions with all their flaws: a biased algorithmic system can still be fairer than an even more biased human decision-maker. In many cases, the best solution consists in integrating human and automated judgements, by enabling the affected individuals to request a human review of an automated decision as well as by favouring transparency and developing methods and technologies that enable human experts to analyse and review automated decision making. In fact, AI systems have demonstrated an ability to successfully also act in domains traditionally entrusted the trained intuition and analysis of humans, such as medical diagnosis, financial investment, the granting of loans, etc. The future challenge will consist in finding the best combination between human and automated intelligence, taking into account the capacities and the limitations of both."

Lawful bases

The ICO provides some useful guidance to help organisations decide which lawful bases to rely on when processing personal data using AI, including recommending that it may be appropriate to choose different lawful bases for your AI development and deployment.

Algorithmic audits and governance measures

The European Commission's 'Ethics guidelines for trustworthy AI' (2019) provide a useful framework for considering the ethical issues that come into designing and implementing AI systems.

In terms of trying to find a solution to eliminate bias in AI systems, algorithmic audits may play a key role by identifying the factors that influence an algorithmic decision. The ICO have said in their AI guidance:

"The idea is that auditability should be 'baked in' to algorithms in the development stage to enable third parties to check, monitor, review and critique their behaviour. For companies in the private sector the concept of an algorithmic audit is likened to an accounting audit which, while carried out in confidence to protect proprietary information, can still provide public assurance."

Those audit procedures themselves also need to be transparent.

Audits should be used in tandem with other governance measures such as ethics boards set up to highlight areas of potential ethical concerns and suggest possible resolutions, and consultation with stakeholders, including those at risk of being adversely affected by an AI system. Approaches like a holistic approach to Corporate Digital Responsibility may help (see https://corporatedigitalresponsibility.co.uk/).

Highlights of the guidance from the European bodies and regulators

European Commission:

The Commission has published:

- a whitepaper on AI (2020): https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en
- Ethics guidelines for trustworthy AI (2019): https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
- its Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act): https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (draft AI Regulation)
- its proposal for a new Machinery Regulation, covering a wide range of machinery products such as 3D printers and robotics, and ensuring that AI systems are safely integrated into the overall machinery: https://ec.europa.eu/docsroom/documents/45508

The draft AI Regulation will notably:

- create a new framework of regulators, monitoring and testing, compliance obligations and governance;
- ban use of AI systems that produce an unacceptable risk to individuals (particularly if there is a safety impact or people's livelihoods are affected);
- subject high-risk AI systems (including remote biometric ID systems) to **strict obligations** before they can be released, including regarding risk assessment, dataset quality, audit logs, human oversight and security; and
- for the most serious infringements, introduce maximum administrative fines of up to €30,000,000 or, for corporate offenders, up to 6% of its total worldwide annual turnover for the preceding financial year, whichever is higher

Council of Europe

The Council has published a Report on Artificial Intelligence Artificial Intelligence and Data Protection: Challenges and Possible Remedies (2019): https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

European Parliament:

The European Parliament has published:

1. a study on the impact of GDPR on artificial intelligence (2020): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf
2. a briefing on the impact of GDPR on artificial intelligence: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530(ANN1)_EN.pdf

European Data Protection Supervisor (EDPS):

The EDPS has published an Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust (Opinion 4/2020): https://edps.europa.eu/sites/default/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

European Union Agency for Fundamental Rights (FRA):

In its 2020 report, the FRA:

1. provides some useful examples of theoretical assessment of harm and significant impact of AI or automated decisions in the areas of social welfare, predictive policing, medical diagnosis and targeted advertising;
2. says that we can learn from DPIAs; and
3. calls on the EDPB and EDPS to issue further guidance.

"The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) should consider providing further guidance and support to effectively implement GDPR provisions that directly apply to the use of AI for safeguarding fundamental rights, in particular as regards the meaning of personal data and its use in AI, including in AI training datasets. There is a high level of uncertainty concerning the meaning of automated decision making and the right to human review linked to the use of AI and automated decision making. Thus, the EDPB and the EDPS should also consider further clarifying the concepts of 'automated decision making' and 'human review', where they are mentioned in EU law. In addition, national data protection bodies should provide practical guidance on how data protection provisions apply to the use of AI. Such guidance could include recommendations and checklists, based on concrete use cases of AI, to support compliance with data protection provisions."

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

ENISA:

The European Union Agency for Cybersecurity (ENISA) has published a report on Artificial Intelligence Cybersecurity Challenges (2020): https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

UK (ICO):

The ICO has the following guidance on AI and data protection:

1. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
2. ICO guidance on AI and data protection

France (CNIL):

The French CNIL has published various guidance:

1. https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues
2. Recommendations on algorithms and discrimination
3. https://www.cnil.fr/sites/default/files/atoms/files/cnil_white-paper-on_the_record.pdf (on voice assistants)

Italy (Garante):

The Garante has opened an investigation into the use by a company of "Deep Fake" type technology that "undresses" women (available only in Italian): https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9470722 (2020)

Norway (Datatilsynet)

The Datatilsynet has published a guide on AI and privacy (English version): https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

It is also launching a regulatory sandbox for the development of responsible artificial intelligence (in Norwegian): https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/regulatorisk-sandkasse-for-utvikling-av-ansvarlig-kunstig-intelligens/

Spain (AEPD)

The AEPD has published guides on:

1. the incorporation of GDPR within processing activities using artificial intelligence technologies (2020) (English version): https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia-en_0.pdf
2. controls to implement for conducting audits of personal data processing that involve artificial intelligence components (2021) (in Spanish): https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf

Key takeaways for businesses developing and using AI-driven technologies:

1. Consider AI in its proper context – whilst AI is moving forward at a rapid rate and its potential is massive, true AI is still a developing technology.
2. Ensure your solution complies with data protection laws, and in time purpose-built AI legislation – existing data protection requirements will need to be complied with, such as the data protection principles, fairness, accountability, transparency and data subject rights, but watch this space for the EU's new regulatory framework on AI.
3. Do proper due diligence on any potential vendor or provider. Don't be fooled by sales spiel and make sure

that any solution you are being offered does what is being promised, is offered by a reputable supplier and addresses any compliance concerns.

4. Keep on top of the available guidance – there is a high volume of guidance in this area, and expect more to come in future as this area develops further.
5. Ensure that adequate safeguards are in place to protect people from biased or discriminatory decisions or outcomes – these should leverage the best aspects of both human and automated intelligence.
6. Ensure that ethical considerations are given sufficient weight – just because you have the technical capability do something, does not necessarily mean that you *should*.
7. Do a proper DPIA, consult with specialist lawyers as appropriate and build time into your development schedules to assess the risks properly.

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav

For more information please contact Katherine Eyres or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Office: +44 (0)207 075 1784

jonathan.armstrong