GIBSON DUNN

February 26, 2020

EU PROPOSAL ON ARTIFICIAL INTELLIGENCE REGULATION RELEASED

To Our Clients and Friends:

On February 19, 2020, the European Commission ("EC") presented its long-awaited proposal for comprehensive regulation of artificial intelligence ("AI") at European Union ("EU") level: the "White Paper on Artificial Intelligence – A European approach to excellence and trust" ("White Paper").[1] In an op-ed published on the same day, the president of the EC, Ursula von der Leyen, wrote that the EC would not leave digital transformation to chance and that the EU's new digital strategy could be summed up with the phrase "tech sovereignty."[2]

As anticipated in our 2019 Artificial Intelligence and Automated Systems Annual Legal Review, the White Paper favors a risk-based approach with sector and application-specific risk assessments and requirements, rather than blanket sectoral requirements or bans. Together with the White Paper, the EC released a series of accompanying documents, including a "European strategy for data" ("Data Strategy")[3] and a "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics" ("Report on Safety and Liability").[4] The documents outline a general strategy, discuss objectives of a potential regulatory framework and address many potential risks and concerns related to the use of AI and data. The White Paper is thus the first step to start the legislative process, which was announced by EC president Ursula von der Leyen at the beginning of her presidency.[5] Currently, it is expected that the draft legislation, which is part of a bigger effort to increase public and private investment in AI to more than €20 billion per year over the next decade,[6] will become available by the end of 2020.

We discuss the key contents of the White Paper, the Data Strategy and the Report on Safety and Liability below, focusing on those topics that would have the most significant impact on technology companies active in the EU, if they were enacted in future legislation.

I. WHITE PAPER ON ARTIFICIAL INTELLIGENCE

The White Paper is the centerpiece of a package of measures to address the challenges of AI. It sets out different policy options with the "twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology." The White Paper, which is a document used by the EC to launch a debate with the public, stakeholders, the European Parliament and the Council in order to reach a political consensus, is structured into two parts: (1) The first part sets out more political and technical aspects to promote a partnership between the private and the public sector in order to form an "ecosystem of excellence" and (2) the second part proposes key elements of a future regulatory framework for AI to create an "ecosystem of trust".

While the first part of the White Paper mostly contains general policy proposals intended to boost AI development, research and investment in the EU, the second part outlines the main features of a possible regulatory framework for AI. In the EC's view, lack of public trust is one of the biggest obstacles to a broader proliferation of AI throughout the EU. Thus, as we have discussed previously,[7] similar to the General Data Protection Regulation ("GDPR"), the EC intends for the EU to maintain its "first out of the gate" status and increase public trust by attempting to regulate the inherent risks of AI. The main risks identified by the EC concern fundamental rights (including data privacy and non-discrimination) as well as safety and liability issues. Apart from possible adjustments to existing legislation, the EC concludes that a new regulation specifically on AI is necessary to address these risks.

According to the White Paper, the key issue for any future legislation would be to determine the scope of its application. The assumption is that any legislation would apply to products and services relying on AI. Furthermore, the EC identifies "data" and "algorithms" as the main elements that compose AI, but also stresses that the definition of AI needs to be sufficiently flexible to provide legal certainty while also allowing for the legislation to keep up with technical progress.

In terms of substantive regulation, the EC favors a context-specific risk-based approach instead of a GDPR "one size fits all" approach. An AI product or service will be considered "high-risk" when two cumulative criteria are fulfilled:

(1) **Critical Sector**: The AI product or service is employed in a sector where significant risks can be expected to occur. Those sectors should be specifically and exhaustively listed in the legislation; for instance, healthcare, transport, energy and parts of the public sector, such as the police and the legal system.

(2) **Critical Use:** The AI product or service is used in such a manner that significant risks are likely to arise. The assessment of the level of risk of a given use can be based on the impact on the affected parties; for instance, where the use of AI produces legal effects, leads to a risk of injury, death or significant material or immaterial damage.

If an AI product or service fulfils both criteria, it will be subject to the mandatory requirements of the new AI legislation. However, additionally, the use of AI based applications for certain purposes should always be considered high-risk when they fundamentally impact individual rights. This could include the use of AI for recruitment processes or for remote biometric identification (such as facial recognition). Moreover, even if an AI product or service is not considered "high-risk", it will remain subject to existing EU-rules such as the GDPR.[8] Notably, the EC expressly takes the view that the GDPR already regulates all issues related to personal data.

Taking into account the "Ethics Guidelines for Trustworthy Artificial Intelligence" of the High Level Expert Group on Artificial Intelligence,[9] the EC sets out six key requirements, which could be included in the upcoming AI legislation:

1. Training Data

The EC proposes several requirements related to training data, such as a requirement to train AI systems on data sets that are sufficiently broad and representative, as well as a requirement to ensure that privacy and personal data are adequately protected during the use of AI-enabled products and services. Further, the adequate protection of personal data during the use of AI products and services should be ensured.

2. Data and Record-keeping

In light of the complexity and opacity of many AI systems, the EC recommends that the regulatory framework prescribe the keeping of accurate records regarding the data set used to train and test the AI systems (including a description of the main characteristics and how the data set was selected), the retention of the data sets themselves and the documentation on the programming and training methodologies, processes and techniques used to build, test and validate the AI systems. The records, data sets and documentation would have to be retained during a limited, reasonable time period to enable effective enforcement and regress of potential victims. Where necessary, arrangements should be made to ensure that confidential information, such as trade secrets, is protected.

3. Information Provision

In the EC's view, transparency requirements, such as ensuring clear information regarding the AI system's capabilities and limitations and informing individuals when they are interacting with an AI system and not a human being, could also be considered. However, no such information would need to be provided in situations where it is immediately obvious to the user that they are interacting with AI systems.

4. Robustness and Accuracy

To minimize the risk of harm, the EC suggests that the regulatory framework should require that AI systems are robust and accurate, that their outcomes are reproducible, that they can adequately deal with errors or inconsistencies throughout all life cycle phases, and that they are resilient against both overt and more hidden attacks.

5. Human Oversight

The EC recognizes that the appropriate degree of human oversight to ensure that AI systems do not undermined human autonomy or cause other adverse effects may vary from case to case. For example, the rejection of an application for social security benefits may be decided upon by an AI system, but should become effective only subject to human review and validation; conversely, the rejection of an application for a credit card may be taken by an AI system with the possibility of subsequent human review. Additionally, operational blocks could be built into the AI system in the design phase, for instance an automatic stop for a driverless car when the conditions do not permit the safe operation of the car.

6. Specific Requirements for Remote Biometric Identification

As we have discussed recently,[10] the EC considered a five-year ban on the use of facial recognition technology in public spaces. Instead, without providing any clear time frame, the EC now intends to launch a broad public debate on the specific circumstances which might justify the use of remote biometric identification and on possible safeguards to be employed.

The White Paper also addresses personal and geographic scope of the future AI legislation. Since many actors may be involved in the lifecycle of an AI system (developers, producers, distributers, end-users, etc.), it is proposed that obligations under the future legislation should be distributed among the different actors based on who would be best placed to address the respective risks. Regarding geographic scope, the EC emphasizes that the objectives of the legislative may only be achieved if the requirements set out in the future legislation apply to all companies providing AI based products or services in the EU, regardless of their actual location.

In terms of compliance and enforcement, the EC favors a mandatory prior conformity assessment for all providers of high-risk AI applications to verify compliance with the above mentioned criteria. This could include checks of the algorithms and of data sets used during the development phase. The *ex post* enforcement of the new requirements as well as the *ex ante* conformity assessment could be entrusted to existing governance bodies in the individual EU Member States and an overarching European governance structure.

Finally, the White Paper proposes the introduction of a voluntary labelling scheme for non "high-risk" AI applications, where interested parties would be awarded with a quality label for their AI products and services.

II. DATA STRATEGY

The Data Strategy presents policy measures aiming to foster a European "data economy" within the next five years. As already evident by the EC's focus on Big Tech firms in the area of antitrust, the EC continues this trend by trying to break the dominance of US and Chinese tech firms with new proposals including the option to introduce a compulsory "data access" right for competitors.[11] In a statement during the presentation of the Data Strategy, the European Commissioner for the Internal Market, Thierry Breton, said that the EU had missed the battle for personal data, but the "battle for industrial data starts now."[12]

To achieve this aim, the Data Strategy recommends to create a single European data space[13] and identifies several issues, such as the fragmentation of legal frameworks between EU Member States, the availability of quality data, and imbalances in market power and data infrastructures that are currently impeding the EU's ability to take a leading role in the global data economy. To overcome these challenges, the EC lists a number of proposals which focus on creating a legal framework, building the necessary infrastructure and honing in on the vast potential of non-personal "industrial data." This also includes the possibility for non-European companies to access and use EU data, provided they comply with the applicable laws and standards.

Specifically, the EC's Data Strategy is based on four pillars, which include concrete proposals for regulatory action:

1. Introduction of a cross-sectoral legislative framework for data access and use

According to the EC, a legislative framework for the governance of common European data spaces will be put into place in Q4 2020. This framework could include standardization mechanisms and harmonized description of datasets to improve both data accessibility and interoperability between sectors in line with so-called "FAIR principles", namely Findability, Accessibility, Interoperability and Reusability. Further, the EC intends to move forward with the adoption of an implementing act on high-value data sets under the Open Data Directive[14] in Q1 2021 in order to make available key public sector reference data in machine-readable format. Finally the EC is contemplating a new "Data Act" to be introduced in 2021 which would provide incentives for horizontal data sharing across sectors and could include a "data access" right for competitors, as described above. Further regulatory action includes an update of the Horizontal Co-operation Guidelines[15] to provide more guidance to companies on the compliance of data sharing and pooling arrangements with EU competition law, a review of jurisdictional issues related to data and - possibly - the explicit regulation of the online platforms economy which is currently being analyzed by the EC's "Observatory on the Online Platform Economy."[16]

2. Investments in data and infrastructures for hosting, processing and using data and interoperability

In order to create an environment in which data-driven innovation is fostered, the EC plans to invest in a project on European data spaces and federated cloud infrastructures. Drawing upon public and private sources, the EC hopes to gather funding in the amount of €4 to 6 billion, of which the EC wants to contribute €2 billion. In March 2020 the EC will present a wider set of strategic investments in new technologies, such edge computing, quantum computing, cyber-security and 6G networks, as part of its industrial strategy. Additionally, the EC promises to bring together a coherent framework around the different applicable rules for cloud services, in the form of a cloud rulebook by Q2 2022 and to introduce a cloud services marketplace for EU users by Q4 2022.

3. Strengthening the digital rights of individuals

Through this initiative the EC is considering the development of "personal data spaces" for individuals. According to the EC, individuals should be in control of their data at "a granular level", to be achieved by enhancing the data portability right under the GDPR, introducing stricter requirements on interfaces for real-time data access and creating a universally usable digital identity. These issues will be explored in the context of the Data Act that could be introduced in 2021.

4. Development of common European data spaces in strategic sectors

Finally, the EC envisions the development of nine common European data spaces across strategic sectors, including the industrial/manufacturing, transport/logistics, healthcare, financial services, energy and agricultural sectors. The idea is to create large pools of industrial data, combined with the necessary infrastructure, to use and exchange data as well as appropriate governance mechanisms. Although these data spaces mainly concern industrial data, the EC emphasizes that they will be developed in full compliance with data protection rules and the highest available cyber-security standards.

III. REPORT ON SAFETY AND LIABILITY

The EC's Report on Safety and Liability, which also accompanies the White Paper, analyses the EU's current product safety and liability legislation.[17] It determines that the existing EU horizontal and sector-specific legislative framework is robust and reliable, since the current definition of product safety already includes an extended concept of safety, and that liability issues are generally covered by the liability concept already in place. However, the EC also identifies certain gaps with respect to the legal management of specific risks posed by AI systems and other digital technologies that should be covered in future product safety and product liability legislation.

In light of the recommendations contained in the Report on Safety and Liability, future **product safety legislation** may cover, *inter alia*, the following aspects:

- **Connectivity and cyber vulnerabilities**: Product connectivity, interconnectivity and interaction of products with other devices may compromise the safety of the product directly and indirectly (e.g., when a product is hacked). Thus, the EC recommends the adoption of explicit provisions such as an explicit assessment of the risks which stem from interconnectivity in order to provide better protection of users and more legal certainty.

- **Autonomy**: Unintended outcomes based on the use of AI could cause harm to users and exposed persons. In order to improve the safety of users, the EC takes inspiration from sector-specific laws to recommend the adoption of horizontal legislation that obliges the appropriate economic operator (i.e. the manufacturer, the distributor or the software producer) to carry out new risk assessment procedures during the products' lifetime. Furthermore, the EC suggests the adoption of specific requirements to ensure human oversight of AI products and systems, starting from their design throughout their lifecycle.

- **Mental health risks**: The EC anticipates that the behavior of AI applications may generate mental health risks and harm, which should be explicitly covered by the definition of product safety in future legal frameworks. In particular, legislation in this field should cover vulnerable users, such as elderly persons in care environments.

- **Data dependency**: Risks to safety may result from a product's faulty collection or processing of data, including a lack of accuracy or relevance. Against this backdrop, the EC recommends that

EU product safety legislation should address the risks of faulty data at the product design stage as well as throughout the entire lifecycle.

- **Opacity**: With regard to the "black-box effect" in the decision-making processes of AI systems, the EC has identified a possible new challenge for product safety ex-post enforcement mechanisms that is not covered by existing legislation. The EC therefore suggests considering transparency requirements for algorithms, as well as requirements for robustness, accountability and human oversight of decision-making. This could include imposing obligations on developers of algorithms to disclose design parameters and metadata of datasets in case accidents occur.

- **Software**: While EU product safety legislation may cover risks stemming from software integrated into a product or device, the EC proposes to adapt and clarify existing rules in the case of stand-alone software placed on the market as it is or downloaded into a product after its placement on the market (e.g. an app that is downloaded on a mobile device). In particular, this would concern stand-alone software that has an impact on the safety of an AI product or system.

- **Complex value chains**: EU product safety legislation imposes obligations on several economic operators following the principle of "shared responsibility". However, the EC suggests that provisions specifically requesting cooperation between economic operators in the supply chain and users should be adopted. For example, each actor in the value chain who has an impact on the product's safety, from software producers to repairers modifying the product, should assume responsibility and provide the next actor in the chain with the necessary information and measures.

In light of the recommendations contained in the Report on Safety and Liability, future **product liability legislation** may cover, *inter alia*, the following aspects:

- **Complexity of products, services, and the value chain**: The EC considers the definition of "product" in the current Product Liability Directive to be sufficiently broad to cover AI products and systems. However, in the view of the EC, the scope of the Product Liability Directive should be clarified to reflect the complexity of such products and systems and to ensure that compensation is always available for damage caused by products that are defective because of software or other digital features.

- **Burden of proof in complex environments**: The current liability regime in the EU relies on the parallel application of the Product Liability Directive, which features a system of strict liability, and fault-based and/or strict liability rules of the individual EU Member States. In order to mitigate the consequences of complexity, the EC is seeking industry feedback whether and to what extent it may be necessary to alleviate or reverse the burden of proof required by the individual EU Member State's liability rules for damage caused by the operation of AI applications. For instance, a reversal as regards fault and causation could apply where the relevant economic operator failed to meet specific mandatory cyber-security or other safety rules.

- **Connectivity and openness**: Connectivity and openness characteristics of AI products may influence the safety expectations with regard to damage that results from cyber-security breaches.

Furthermore, connected products may also be used for purposes beyond those reasonably expected by the manufacturer. Therefore, the EC considers legislation in order to clarify and facilitate compensation for damages caused to users, particularly in situations concerning foreseeable reasonable use and contributory negligence (e.g., the failure of the injured party to download a safety update).

- **Autonomy and opacity**: In addition to issues such as complexity, the fact that AI applications can improve their performance by learning from experience creates a challenge to the effective enforcement of liability claims. The EC notes that a guiding principle for EU product safety and product liability remains the obligation of producers to ensure that all products put on the market are safe throughout their entire lifecycle and for the use that can reasonably be expected. In order to address the remaining uncertainties regarding the liability of manufacturers the EC proposes revisiting the notion of 'putting into circulation' that is currently used by the Product Liability Directive to cover products that have been changed or altered, and to clarify who is liable for any changes that are made to the product.

- **High-risk applications**: The EC is seeking views on whether and to what extent strict liability, as it exists in some national laws of individual EU Member States, may be necessary in order for possible victims of high-risk AI devices and services (i.e. where there is a possibility of significant harm to important legal interests, like life, health and property) to achieve effective compensation. Further, the EC is also seeking views on whether strict liability should be coupled with an obligation of the relevant economic operator to have in place available insurance. For the operation of non high-risk AI devices and services, the EC suggests that changes to the burden of proof might be required as well, since the victim may not be able to obtain the relevant data required to assess liability from the potentially liable party.

CONCLUSION

While there is no specific draft legislation yet, we expect that the EC will deliver concrete proposals later this year after the public consultation phase has ended. Companies active in the field of AI should closely follow the latest developments in the EU given the proposed geographic reach of the future AI legislation, which is likely to affect all companies doing business in the EU. With the presentation of the White Paper, the Data Strategy and the Report on Safety and Liability, EC President Ursula von der Leyen and her new commission have made it clear that they have ambitious plans for Europe's digital transformation. Certainly we will see a lot of legislative activity in Europe aimed at challenging the US and Chinese dominance in the digital realm, not only with regard to AI. After all, the EC is striving "to export its values across the world"[18] and "actively promote its standards."[19]

As the EC has launched a public consultation period and requested comments on the proposals set out in the White Paper and the Data Strategy, this is an important opportunity for companies and other stakeholders to provide feedback and shape the future EU regulatory landscape for AI. If you are interested in submitting comments, you may do so at https://ec.europa.eu/info/consultations_en until May 19, 2020.

We have been advising clients on regulatory and governance issues in anticipation of such legislative actions in the EU, and we invite anyone interested to reach out to us to discuss these developments.

---

[1] EC, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 (Feb. 19, 2020), *available at* https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[2] EC, *Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission*, AC/20/260, *available at* https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260.

[3] EC, *A European strategy for data*, COM(2020) 66 (Feb. 19, 2020), *available at* https://ec.europa.eu/info/files/communication-european-strategy-data_en.

[4] EC, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 (Feb. 19, 2020), *available at* https://ec.europa.eu/info/files/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en.

[5] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, *available at* https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

[6] EC, *Artificial Intelligence for Europe*, COM(2018) 237 (Apr. 25, 2018), *available at* https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

[7] H. Mark Lyon, *Gearing Up For The EU's Next Regulatory Push: AI*, LA & SF Daily Journal (Oct. 11, 2019), *available at* https://www.gibsondunn.com/wp-content/uploads/2019/10/Lyon-Gearing-up-for-the-EUs-next-regulatory-push-AI-Daily-Journal-10-11-2019.pdf.

[8] The exact implications and requirements of the GDPR on AI based products and services are still not entirely clear, *see further*, Ahmed Baladi, *Can GDPR hinder AI made in Europe?*, Cybersecurity Law Report (July 10, 2019), *available at* https://www.gibsondunn.com/can-gdpr-hinder-ai-made-in-europe/.

[9] For further detail, *see* our 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[10] *See* our 2019 Artificial Intelligence and Automated Systems Annual Legal Review.

[11] While the exact prerequisites are not yet clear, the EC notes that a data access right should only be made compulsory where specific circumstances require it (i.e. where a market failure in a specific sector is identified or can be foreseen and cannot be resolved by competition law) and where it is appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions.

[12] Samuel Stolton and Vlagyiszlav Makszimov, *Von der Leyen opens the doors for an EU data revolution*, Euractiv (Feb. 20, 2020), *available at* https://www.euractiv.com/section/digital/news/von-der-leyen-opens-the-doors-for-an-eu-data-revolution/.

[13] This is defined in the Data Strategy as "a genuine single market for data, open to data from across the world".

[14] Directive (EU) 2019/1024 of the European Parliament and of the Council of June 20, 2019, OJ L 172, p. 56-83.

[15] European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 2011/C 11/01, OJ C 11, p. 1-72.

[16] *See* https://ec.europa.eu/digital-single-market/en/eu-observatory-online-platform-economy.

[17] The current framework consists of, inter alia: the General Product Safety Directive (Directive 2001/95/EC of the European Parliament and of the Council of Dec. 3, 2001, OJ L 11, 15.1.2002, p. 4-17); specific horizontal and sectorial rules, such as the Market Surveillance Regulation (Regulation (EC) No. 765/2008 of the European Parliament and of the Council of July 9, 2008, OJ L 218, 13.8.2008, p. 30-47, and the Machinery Directive (Directive 2006/42/EC of the European Parliament and of the Council of May 17, 2006, OJ L 157, p. 24-86); and the Product Liability Directive (Directive 85/374/EEC of July 25, 1985).

[18] *Supra* note 1, EC, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, p. 9.

[19] *Supra* note 3, EC, *A European strategy for data*, p. 24.

The following Gibson Dunn lawyers prepared this client update: H. Mark Lyon, Michael Walther, Alejandro Guerrero, Selina Grün and Frances Waldmann.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Artificial Intelligence and Automated Systems Group:

Artificial Intelligence and Automated Systems Group:
H. Mark Lyon - Chair, Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33 180, mwalther@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Selina X. Grün - Munich (+49 89 189 33-180, sgruen@gibsondunn.com)
Frances A. Waldmann - Los Angeles (+1 213-229-7914,fwaldmann@gibsondunn.com)
J. Alan Bannister - New York (+1 212-351-2310, abannister@gibsondunn.com)

Ari Lanin - Los Angeles (+1 310-552-8581, alanin@gibsondunn.com)
Robson Lee - Singapore (+65 6507 3684, rlee@gibsondunn.com)
Carrie M. LeRoy - Palo Alto (+1 650-849-5337, cleroy@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

© 2020 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.