Cybersecurity Law Report
An Acuris company

cslawreport.com

July 10, 2019

GDPR

Can GDPR Hinder AI Made in Europe?

By Ahmed Baladi, *Gibson, Dunn & Crutcher*

One year after the GDPR became enforceable, it is clear that it has had impressive repercussions around the globe. It is difficult to identify any other E.U. regulation that has generated so much concern and attention outside E.U. borders. Multinational organizations and their boards, whether located within the E.U., the U.S. or in Asia, have all taken the GDPR requirements very seriously and invested time and resources to comply with them. GDPR compliance may affect how Europe can compete in the global AI race, however, and clearer regulatory guidelines are needed.

See "Regulating AI: U.S., E.U. and Industry Laws and Guidance" (Oct. 17, 2018).

GDPR's Positive Impact

There is no doubt that the extraterritoriality of the GDPR has been an incredible and unexpected success. This is illustrated by the fact that many organizations operating from outside of the E.U. have realized and acknowledged that the provisions of the GDPR are applicable to them if they satisfy one of the conditions set out in its Article 3 (*i.e.*, if they process personal data related to the offering of goods or services to individuals in the E.U. or if they monitor individuals' behavior in the E.U.).

The other factor that contributed to the GDPR's exposure abroad was undoubtedly the level of potential sanctions to which organizations were exposed. Indeed, the risk of being sanctioned up to 20 million euros or 4 percent of the worldwide annual turnover, whichever is higher, has constituted a real game-changer. This change needs to be confirmed with GDPR enforcement actions, although the French data protection authority seems to have already set the tone by imposing the highest administrative fine under the GDPR to date against Google LLC, with a sanction amounting to 50 million euros on January 21, 2019. This amount is still far from the 4 percent of the worldwide annual turnover but represents an increase of almost 5,000 percent of the previous fines in the E.U. under the former privacy legal framework (Directive EC 95/46). This also demonstrates that the E.U. can adopt the same strategy as the U.S. when applying and enforcing its regulations against overseas companies.

Most importantly, the GDPR has become a global inspiration for lawmakers that have adopted or are considering drawing up similar privacy laws in Brazil, India, China, California, etc. Equally key, the GDPR has led companies to agree to new terms with their clients, wherein they commit to protecting their clients' personal data and acting in a more transparent manner.

Another success to add to the GDPR's credit is the rights newly granted to individuals, which has generated greater interest in the consumer and privacy rights sphere. The increasing number of complaints and legal actions that were prompted by the regulation illustrates that trend.

See CSLR's three-part series analyzing early GDPR enforcement: "Portugal and Germany" (Jan. 23, 2019); "U.K. and Austria" (Jan. 30, 2019), "France" (Feb. 6, 2019).

The Rise of AI

Despite the GDPR's success, it is notable that it is neutral when dealing with a specific technology or innovation. Lawmakers are often taking the risk of adopting regulations that may not be up to date or up to speed with the evolution of technology, and this risk is particularly valid for the GDPR with regard to artificial intelligence.

See "Understanding the Intersection of Law and Artificial Intelligence" (May 30, 2018).

Importance of AI

Before assessing such risk, it is important to understand why AI is so vital.

AI has become an area of strategic importance and a key driver of economic development. AI will indeed impact society and the economy across all industries, from fostering innovation, improving human productivity and curing diseases to transforming human mobility.

Considering the opportunities arising from AI and the socio-economic changes that it will bring, states have designed strategies and investment plans to promote its development. Indeed, the challenge for governments is to maintain and increase their leadership in innovation, or at least limit the gap with the most advanced countries. In this battle, there are clearly two front-runners, China and the U.S., whereas Europe is still fighting to stay in the race.

There are many factors that can influence the results of the race, such as countries' IT and technology base, level of education and training, political will and level of financial investments, but, more importantly, the conditions of access to data and the applicable legal environment.

Efforts to Put the E.U. at the Forefront

The European Commission is conscious of the strategic innovation battle and is working towards putting the E.U. at the forefront. In 2018, the European Commission set out its vision for an "ethical, secure and cutting-edge AI made in Europe" and, for that purpose, it established the High-Level Expert Group on Artificial Intelligence, which published its "Ethics Guidelines for Trustworthy AI" in May 2019.

This working group is definitely addressing some of the factors for success mentioned above. Yet, by focusing its attention on a limited number of issues arising from AI without assessing the level of compatibility between the E.U. legal framework and the development of AI, the E.U. Commission could lose the battle.

It is unfortunate to note that neither the "Ethics Guidelines for Trustworthy AI" nor any other E.U. Commission publication has determined whether it is possible to develop, promote and use AI technology made in E.U. while ensuring strict compliance with the GDPR's requirements. Paradoxically, the

"Ethics Guidelines for Trustworthy AI" even intentionally exclude the question despite its relevance and the urgency of the situation.

The Risks GDPR Poses to Innovation

Regulatory pressure poses relevant challenges at a time when we are laying the foundations for a future in which self-driving cars, humanoid robots, earlier cancer detection, smart assistants or recruiting algorithms won't make headlines. So, does GDPR enable or restrain Europe's development in the era of AI?

See "Regulating AI: U.S., E.U. and Industry Laws and Guidance" (Oct. 17, 2018).

Data Leads to Incompatibility

Technologies such as machine learning need a substantial volume of data to operate, whether they are being used to assist human intervention or in a completely autonomous manner. In most, if not all, cases, the massive volume of data collected and processed for AI solutions also originates from multiple sources and contains personal data (*i.e.*, data related to an identified or identifiable individual). Accordingly, if one of the conditions of Article 3 of the GDPR is satisfied (*i.e.*, if the AI solution is used or developed by an entity established in the E.U., contains personal data resulting from the offering of goods or services to individuals in the E.U. or contains data resulting from the monitoring of an individual's behavior in the E.U.), the development and use of AI solutions is likely subject to the GDPR's onerous obligations, which may, in some cases, result in practical incompatibility.

Unbalanced Competition

One could try to avoid the application of the GDPR's requirements by developing or using an AI solution that does not trigger the application of the GDPR. We can easily imagine a Chinese AI company established in China, or any other jurisdiction located outside the E.U., that relies exclusively on personal data related to individuals who are not in the E.U. In the same manner, its U.S. competitor could manage to avoid the application of the GDPR to conduct its research on an AI solution by undertaking the same steps.

On the contrary, however, any company established in the E.U., irrespective of its corporate size (from a start-up to a multinational organization) or the purpose of its project (whether for health purposes or purely marketing purposes), will have to deal with the GDPR's onerous requirements, hence creating an unbalanced competition with its U.S. and Chinese counterparts. Although the anonymization of personal data in order to avoid the application of the GDPR is frequently highlighted, the reality is that it is highly likely that organizations will not pass the test of an irreversible anonymization process.

Relevant GDPR Requirements

Below are some examples that illustrate the lack of compatibility between GDPR and AI.

See "Irish DPC Helen Dixon on GDPR Enforcement Hurdles One Year In" (May 29, 2019).

Challenges to Obtaining Consent or Supporting a Legitimate Interest

One of the first requirements of the GDPR is to process personal data lawfully. Such processing will typically require an individual's prior consent, which shall be "freely given, specific, informed and unambiguous," and can be withdrawn at any time. One can easily imagine that in the context of AI, where the amount of data at stake is colossal and where anticipating the purposes of the data's use is challenging, obtaining such a prior consent is not always achievable.

On the contrary, by attempting to satisfy such requirements, there is a risk that the opposite result will be achieved if an individual ticks a box at the bottom of the page in order to continue benefiting from the services or products, without taking the time to understand the purpose and effect of the underlying AI technology. One could argue that instead of trying to obtain consent, organizations could rely on a having legitimate interest in the use of the data, which is another legal basis contemplated by the GDPR. Unfortunately, data protection authorities are quite reluctant to admit that such legitimate interest forms a valid legal basis, and even more so when it relates to AI.

Challenges to Meeting Purpose Limitation and Data Minimization Requirements

Other GDPR requirements, like purpose limitation and data minimization, also seem to contradict the use of AI technology, which highly depends on the constant collection and reuse of data.

The principle of purpose limitation is expressed in Article 5(1)(b) of the GDPR, which provides that: "Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes." This principle has a twofold scope. On one hand, personal data can only be processed for purposes that are specified, explicit and legitimate. On the other hand, the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the organization, after having met all of the requirements for the lawfulness of the original processing, should take into account, *inter alia*, the:

- context in which the personal data have been collected, in particular the reasonable expectations of individuals as to its further use;
- consequences of the intended further processing for data subjects; and
- existence of appropriate safeguards in both the original and intended further processing operations.
- In the context of AI, where it is difficult to anticipate the purposes for which data will be used, satisfying the GDPR's purpose limitation tends to be highly impracticable.

The data minimization principle, the idea that the organization should only process the personal data that it actually needs to process in order to achieve its processing purposes, is expressed in Article 5(1)(c) of the GDPR. Considering the volume of data required to develop and operate an AI solution this provision also seems contradictory.

GDPR Requirements Specific to AI

The foregoing challenges should not mask the interesting GDPR provisions that seem geared to AI. The following requirements, to name a few, constitute suitable safeguards to be further tested in the context of AI cases:

- security, which requires ensuring the protection of personal data against unauthorized or unlawful processing and against loss, destruction or damage;
- transparency, which requires informing individuals in clear and plain language of the processing operations that will be undertaken on their personal data as well as the risks, rules, safeguards and rights in relation to such processing operations; and
- data subject rights, which provide individuals with the right to decide how their data gets processed (including the right to have an AI solution reviewed by human intervention) and the right to object to such processing.

Potential Resolution

Despite the considerable consensus on the progress and benefits that would arise from AI and the need to promote trustworthy technology, there is a strong need to resolve, at the continental level, the conflicts between the GDPR and AI.

Develop Guidelines

Resolving such conflict does not necessarily mean adopting a new regulation, which would take too much time and would, in any event, be an impediment to keeping pace with the booming digital transformation. However, what is achievable within a reasonable time is to devise with the E.U. institutions clear and practical guidelines to help AI stakeholders in the E.U. understand the concrete requirements applicable to developing, testing, deploying and using their innovative solutions with sufficient legal confidence.

In order to be pragmatic while ensuring a minimum level of protection to individuals, case-by-case solutions should be preferred to a one-size-fits-all approach. Indeed, one could easily understand that a start-up at the design stage of its AI solution should not be required to cover the entire spectrum of the GDPR requirements.

Assess Risk

The purpose of the AI solution should also be taken into consideration in the risk assessment. A fully automated profiling solution that excludes individuals from an employment position or denies them a right is different from an AI solution that aims to improve a medical diagnosis or cure a disease.

When assessing risk, the nature of the processing operations should be considered. Relying on massive combinations of personal data from multiple sources without being able to track such sources could raise more concerns than dealing with a single source of personal data.

See "How to Improve Risk Analysis in the Wake of the Anthem's Record Settlement" (Nov. 7, 2018).

Consider Technology Safeguards

Technology could actually be helpful in offering appropriate safeguards. We could, for instance, envisage relying on blockchain technology to track sources and data flows in order to facilitate the compliance of AI technology with the GDPR's most fundamental principles (transparency, security, data subjects' rights).

See "Using Technology to Comply With the GDPR" (Feb. 14, 2018); and our three-part series on blockchain technology: "Basics of the Blockchain Technology and How the Financial Sector Is Currently Employing It" (Jun. 14, 2017); "How Financial Service Providers Can Use Blockchain to Improve Operations and Compliance" (Jun. 28, 2017).

Ultimately, there needs to be a solution that resolve the conflicts between the GDPR's requirements and the use and innovation of AI. Failing to help AI stakeholders with pragmatic solutions and guidelines could hamper the European Commission's objectives and weaken E.U. potential to compete on the global stage with U.S. and Chinese counterparts.

Ahmed Baladi is co-chair of Gibson, Dunn & Crutcher's privacy, cybersecurity and consumer protection practice group and based in Paris. He specializes in data privacy and cybersecurity as well as digital transactions, in particular in relation to IoT, AI and Fintech.