WHAT LIES AHEAD WITH THE APPROVED GENERAL DATA PROTECTION REGULATION (GDPR) ?

FOCUS ON PROFILING

Profiling consists essentially in collecting data about a person in order to verify that he or she fits into a pre-established pattern - for example, the pattern of a “bad payer” - so that decisions towards this person can be adjusted accordingly - for example, by granting or not granting a requested loan or changing the applicable conditions.

Profiling is not limited to financial activities. It is everywhere. Think about targeted advertising, involving great amounts of data on internet users such as history of visited pages, downloaded applications or social media preferences, in order to send relevant commercials to selected profiles. Or, fraud busting, for which fraud patterns are being developed and refined all the time about employees, or clients, or suppliers in order to issue warnings as soon as the likelihood of fraud is getting higher.

As useful and as relevant as profiling can be, it is sometimes considered as a “dangerous” technique by privacy professionals. The first reason is that it may lead to decisions relying on statistics and likelihood, rather than real-life assessments, and that statistics often have a bad reputation of either being proved wrong, for lack of accuracy, or being manipulated for justifying certain actions. The second reason is that profiling, in certain cases, would bear the risk of stigmatisation against the individuals: because someone has acted in certain way in the past, he/she would be blacklisted and refused a loan, a home or a job, without an opportunity to present a case or obtaining redemption after a certain period.

On the ground that profiling is risky, when poorly designed, and gets used in an increasing number of situations, the General Data Protection Regulation (“GDPR”), as approved by the EU institutions on December 15, 2015, completely revisits the legal approach. We will examine such innovations and try to understand how the legal framework has jumped from near ignorance in the 1995 Directive - only one mention of profiling in the Preamble – to near obsession in the GDPR of 2015, in which we counted no less than twenty provisions addressing this issue.

Transparency

First of all, the GDPR imposes a new obligation on the data controller to provide the data subject with information on the existence of automated decision-making including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This information must be provided by the data controller at the time the data is collected (Article 14) but may also be obtained, at a later stage, by exercising a right of access (Article 15).

Reinforced protection

Under the GDPR (Article 19), data subjects have a right to object to profiling based on the legitimate interests of the data controller, who may then overcome such objection by demonstrating compelling legitimate grounds. Where profiling is used for direct marketing purposes, the objection by the data subject cannot be overridden.

Besides, the Regulation institutes a tailored and specific right, under Article 20, not to be subject to a decision based solely on automated processing, including profiling, when such decision produces legal effects concerning the data subject or significantly affects him/her. Such right,
such prohibition, does not apply if the decision is necessary for a contract between the data subject and the controller, or is authorized by law, or is based on data subject’s explicit consent.

However, in these cases, the data subject will have the right to obtain human intervention, to express his/her point of view and to contest the decision.

**Accountability**

Accountability is one core principle of the GDPR whereby the data controller must be able to demonstrate compliance of its processing activities with the Regulation and the effectiveness of measures implemented for that purpose, in adequacy with the specifics of the processing and the risk for the rights and freedoms of individuals. In this respect, the GDPR makes it clear that data processing which involves profiling must be considered as bearing a significant level of risk. In the Preamble (para. 60a), profiling is indeed cited as possibly leading to physical, material or moral damage of varying severity. As a consequence, Article 33 provides that a privacy impact assessment should be conducted each time an automated processing is implemented, including profiling, which leads to “systematic and extensive evaluation of personal aspects relating to natural persons” and based on which decisions are made “that produce legal effects concerning the individual”

**Increased sanctions**

Infringements of the data subjects’ rights pursuant to Articles 12-20, including those rights based on transparency and the reinforced protection mentioned above, are subject to the maximum available fines of up to EUR 20 million or 4% of the total worldwide annual turnover for the preceding financial year. This constitutes a major change for data controllers who, before the GDPR, were used to five or six-figure-fines depending on their country of establishment.

**Extra-territoriality**

As a final mark of the importance accorded to profiling, the GDPR makes sure that data controllers may not escape the European legal framework by reason of their place of establishment. Indeed, Article 3, read in conjunction with the Preamble (para. 21), indicates that monitoring the behaviour of individuals located in the European Union justifies the application of the Regulation, especially when such monitoring takes the form of profiling to analyse or predict individuals’ preferences, behaviours and attitudes.

Altogether, it appears that profiling is an excellent entry point to understand the new era of data protection inaugurated by the GDPR. It is indeed the best example of the new risk-based approach, the new accountability principle, and the new heightened sanctions.

To know more about detailed implementation, we will now have to wait for the guidance by the European Data Protection Board (Preamble, para. 58a, and Article 66-1).

**Alexandre Entraygues**

Avocat à la Cour  
Cabinet Linklaters