EUROPEAN GENERAL DATA PROTECTION RULE AND IMPACT ON ONLINE ADVERTISING

BAPTISTA LUZ
ADVOGADOS

/ EUROPEAN GENERAL DATA PROTECTION RULE AND IMPACT ON ONLINE ADVERTISING[1]

Pedro Henrique Soares Ramos
Renato Leite Monteiro

At this time of the year, the acronym GDPR should have been heard by everyone in the advertising market since the *General Data Protection Rule* shall be in force throughout the European Union (EU) on May 25. **However, few people may have noticed the impact the GDPR will have on Brazil, as well as the potential changing factor of such general rule in the online advertising sector[2].**

Here are some of the primary GDPR provisions:

(i) The extensive definition of personal data determining that the general rule must be applied to data handling related to an identified or identifiable person, even through cookies, unique identifiers and dissociated data and the joint liability of the controller, or better put, the one responsible for the personal data and the processor.

For sake of clarity, the GDPR carries two different concepts, the *data controller* and the *data processor*. The controller is not necessarily the one controlling the data or providing it, it is only the one determining the destination of the data, its purpose, gathering method, etc. In the case of the advertising market, the controller could be the *publisher* that collects data or the advertiser making it available for media purchase operations, for instance.

The processor carries out the handling measures. Sometimes both entities, controller and processor, are confused.

[1] This article is an expansion of another article titled: "Impact of the European General Data Protection Rule on Brazilian advertising", published in the periodical 'Meio & Mensagem' on 03.01.2018 as written by Pedro Ramos. Article available at: goo.gl/GzNCnC. Accessed on 13.03.2018.

[2] This article is an expansion of another article titled: "Impact of the European General Data Protection Rule on Brazilian advertising", published in the periodical 'Meio & Mensagem' on 03.01.2018 as written by Pedro Ramos. Article available at: goo.gl/GzNCnC. Accessed on 13.03.2018.

Furthermore, the liability of the controller, depending on the measures taken, could be limited to what was determined by data purposes. Therefore, it is not unrestrictive joint and several liability. Additionally, the term *data controller* translated into Brazilian Portuguese would not be a term related to "controller", but "responsible". The *data processor* would be the operator, under Bill 5276/2016, being analyzed at the House of Representatives, which provides for personal data handling in Brazil. One example of processor in advertising would be *AdTech* that will use the data for inventory enhancement;

(ii) A requirement, when possible, to use pseudonymity procedures, for reducing damage risks arising out of an occasional leakage. Pseudonymizing is different from anonymizing personal data. Anonymizing refers to processes that do not allow for new identification or individualization of the entity to whom the data refers. When pseudonymizing, the person handling the data can at least reidentify the data owners by adding such data to the identified data it holds, such as names, CPF (Individual Taxpayers' Registration), RG (ID Cards), emails, etc.

However, in some cases, pseudonymity is not required. For example, in its ad Exchange platform Facebook would not be necessarily obliged to pseudonymize the data handled since it already has the direct identification of many data owners. The platform processes the data internally and returns the results without sharing individualized data;

(iii) Rights to data access, rectification, cancellation, opposition and portability assured to users so that they can transfer their data to other services, even to competitors of the company in possession of such data; and

(iv) A requirement for companies to adopt a high level of compliance using data inventories, maintaining privacy impact reports, legal statement checklists and the appointment of a Data Protection officer, according to the type of data handled as well as the size of the infrastructure.

The impact of the provisions introduced is not limited to the EU: **the GDPR impacts virtually all Brazilian advertising operations** since it provides **extraterritorial effectiveness**. To mention just a few circumstances, if advertiser, publisher or AdTech have their main office, branch or representation in the EU, or if the servers where data is processed are in the EU, or even if the advertiser's services or products are offered to residents in the EU, regardless of their nationality, **the GDPR is applied**.

And when it comes to the GDPR application, we are also referring to excessively high penalties: **the highest fines can reach 20 million Euros or 4% of the global revenue of companies, whichever amount is higher.**

Such impositions bring consequences to one of the most expanding market in the world. **Not only will privacy policies have to be redesigned, but also the entire logic of the business model and its value chain**.

Such modifications have clearly brought a lot of discussion as to how the market would adapt without impairing its development, and one of the main discussion points is how to get the legal grounds (i.e. authorization by GDPR) for data gathering and processing. One of the updates is that **consent by the user is not the only possibility for legal grounds:** the GDPR also provides for some other legal grounds, such as:

(i) Execution of an agreement with the user (e.g. delivering a product acquired on a website);

(ii) Compliance with a legal requirement (e.g. compliance with court orders or a data protection requirement);

(iii) When required to protect elementary rights (e.g. to contact an ambulance service);

(iv) When required for the public interest or for activities of a legally authorized entity (e.g. a data leakage investigation); and

(v) When the controller (or data handling party) has a legitimate interest in using the data for other purposes, which is an open circumstance comprising situations in which consent is hard to obtain even in case of reasonable and proportional handling, not

violating other rights, among them, the "ARCO" rights, even if not of interest to the data holder (e.g. when a debt collection agency uses the data to try to collect the debt).

Since free consent, as required by the GDPR, is difficult to obtain when it comes to online advertising, the sector is expected to be primarily based on legitimate interest to justify its activities, although many European authorities have shown their skepticism in understanding advertising as a legitimate expectation of the user.

The **legitimate interest** tends to be a "**balance**" between **third-party interests** and **data owner interests** (expectations of the processing method and corresponding protective reliefs). Examples: crime prevention, fraud detection, cybersecurity, etc. The "**direct marketing**" may be construed as legitimate, but with certain restrictions. The trend is to consider aggregate analysis for trend reports, ad performance monitoring, post-click monitoring and audience calibration as acceptable, provided that an "**opt-out**" option is given within the **context of a previous relationship**. However, it is not clear if behavioral and programmatic advertising will be construed as legitimate interest.

An example of permitted profiling, which in theory could be based on legitimate interests, even if fully automated: a woman in São Paulo aged between 25 and 35 years, probably interested in fashion and certain clothing items. This scenario also allows the inclusion of the use of certain data to customize the view settings of a website; email address maintenance to prevent new registrations with the same email; traffic analytics to the website; receiving user's personal data through external sources for updating purposes, adapting to the data quality principle.

An example of profiling that could challenge its legitimacy, unless otherwise expressly consented by the owner, and all rights being assured: tracking the user through multiple websites, locations, equipment and services. User should always be informed, freely and provided with an opt-out alternative.

And even, if such uncertainty scenario can bring legal insecurity, **it can also foster innovation and good practices unprecedently in the recent history of interactive media**.

First, **concern for *compliance* in advertising is not only because of the GDPR**. Discussions as to brand safety, transparency and accountability in rendering accounts have been in the market for some years, and many companies have proven to be mature enough to approach such issues to the best interest of their advertisers and consumers.

Second, **concern for privacy is not a consequence of GDPR, rather it is its cause**. Over the last years, there was an expansion in user-tracking and profiling tools. Thus, users became more aware of the issue, with an increase of anonymous browsers, adblockers and transparency tools (such as Ghostery). Furthermore, discussions will probably continue and increase their complexity with the debates involving the ePrivacy Directive, to govern directly the rules for online service use, in addition to the GDPR.

Finally, there are countless initiatives under discussion for compliance with GDPR which could innovate things in the sector, such as:

(i) Development of transparency tools, opt-out and user data control, which can reinforce the grounds on legitimate interest;

(ii) Technological alternatives to obtain and, especially, register user consent in the whole media delivery value chain;

(iii) Enhancement of media real-time bidding tools (RTB), aimed at mitigating possible data leakage;

(iv) Development of a cooperation network between publishers, advertisers, agencies and AdTech, increasing transparency of the risks assumed and creating means (contractual and technical) to mitigate brand exposure;

(v) Use of artificial intelligence and machinery learning tools preventing use of individualized data for statistical profiling of users' groups of interest; and

(vi) Creation, by advertising agencies, of advertising campaigns adding more and more importance to control by user, reinforcing the possibility to apply legitimate interest.

In summary, if some still defend that the GDPR will destroy programmatic advertising and return the sector to the paleolithic, our suggestion is the opposite: **the future of online advertising will inevitably be aimed at personal data protection, and the path towards it goes through innovation of the segment and consolidation of the advertising value in society.**