ELECTORAL PROPAGANDA AND PRIVACY: THE ITALIAN DATA PROTECTION AUTHORITY LAYS DOWN RULES FOR THE ADVERTISING CAMPAIGN

ALESSANDRA FABROCINI

Key-words: electoral campaign - electoral propaganda - italian data protection authority

Category: Legal Area

With the provision n. 96 of 18 April 2019, the Italian Data Protection Authority (Garante Privacy) lays down the rules that political parties and individual candidates are bound to respect in order to guarantee fair processing in respect of electors' personal data in the context of election propaganda.
Electors are constantly subject to the risk of external interference and conditioning. Therefore, in view of the forthcoming European electoral consultations and because of the novelty of the GDPR, the Italian Data Protection Authority considers it necessary to draw attention to the main cases in which personal data may be used by political parties and organisations, promoting and/or supporting committees, and individual candidates for propaganda purposes by respecting data subjects' rights and fundamental freedoms.The Electors' data protection is designed to preserve participation in democratic life and confidence in politics.
The independent administrative authority focuses on the use of political and propaganda messages sent to social network users (such as Facebook and LinkedIn) or on other messaging platforms (such as Skype, Whatsapp, Messenger). This use must be in compliance with data protection rules to ensure the lawfulness of the electors' data processing.
There are data that can be used without consent and data that may be used on the basis of a prior elector's consent.In particular, "informed consent is required to be able to use telephone numbers contained in telephone directories and therefore to make calls or send sms and e-mails. Consent obligation also to be able to process data available on the web, such as, for example: those present in social network and messaging profiles; those taken from forums and blogs; those automatically collected on the internet by special software (web or data scraping); the lists of subscribers to a provider; the data published on websites for specific purposes of corporate, commercial or associative information". Consent is also necessary "for data collected in the exercise of professional activities, business or even within the health profession". The provision refers to the use of so-called "consensual" lists (data collected by prior information and consent) by some parties that acquire them from third parties. This is possible, but whoever intends to use the "consensed" lists must verify that

the legal obligations have been effectively complied with. The same applies to electoral propaganda services provided by third parties in favor of movements, parties, candidates.

On the other hand, there are data that cannot be used in any way. They are the data collected or used for the performance of institutional activities, such as the population register of the resident population; the archives of the civil state; the section electoral lists already used in the seats; lists of members of professional associations and boards; e-mail addresses taken from the national digital domicile index. Also, the data made public on the basis of regulatory acts for purposes of publicity or transparency, such as those present in documents published on the online register; those relating to the results of competitions; those reported in the organizational charts of public offices containing telephone numbers and email addresses. Finally, data collected by holders of elective offices and other public offices cannot be used in the exercise of their elective mandate or institutional activity".

Quickly described the variety of data referred to in the provision being analysed, it is important to focus on the data found on the web. Nowadays, personal data is easily found on the internet; however, this does not mean that such data is freely available or that the processing of such data is authorised for any purpose. The data available on the web (telephone numbers or e-mail addresses) must be processed, in compliance with the principles of correctness and purpose, only for the purposes underlying their publication. Therefore, even with regard to advertising campaign, there is a general prohibition on using the data found on the web for this purpose without a specific informed consent on this purpose.

Regarding the data published on social networks, there are serious risks of improper use of personal data of citizens for profiling and sending massive communications or even to address customized campaigns (micro-targeting). The risk to which voters are subject is to see their political orientation and/or their choice of voting influenced, based on their personal interests, values, habits, and lifestyle. In this context, the political and propagandistic messages sent to social network users (such as Facebook or Linkedin), in private as well as publicly on their virtual bulletin board, are subject to the rules on data protection. The same discipline is also applicable to messages sent using other platforms, such as Skype, WhatsApp, Viber, Messanger.

Electors "must always be informed about the use that will be made of their personal data". The owner, in the light of the principle of accountability, "must take appropriate measures to protect the rights, freedoms and legitimate interests of the interested party, also making information public". Therefore, there is a logic of greater responsibility of the data controller: "it is necessary to adopt adequate technical and organizational measures to ensure that the processing is carried out in compliance with the legislation in force". More specifically, in the light of the new principles of accountability and

privacy by design, who processing data (parties, political movements, committees, individual candidates), prepare adequate organizational and technical measures, such as to guarantee the effective and timely execution of the rights. It is also necessary to be able to prove with appropriate documentation the planned and adopted measures, as well as the evaluation procedure for their identification, including risk assessment.

Finally, the Italian Data Protection Authority points out that the violation of the data discipline entails sanctions that can also be very onerous, as envisaged by the GDPR.

The European Authority could become aware of a decision of a National Data Protection Authority from which it is possible to infer that the violation of the rules is connected to activities that influence the outcome of the European elections for political parties and European political foundations. In this case, the European Authority is required to initiate a verification procedure, at the end of which financial penalties may be applied. In the most serious cases, these penalties could amount to 5% of the annual budget of the party or foundation.

Source: Garante per la protezione dei dati personali

Link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9105208