Full title of law or regulation	Garante: Guidelines on Marketing and against Spam - 4 July 2013 [4304228] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4304228
Title of relevant section	Social Spam 6.1
Introduction	6. New Types of Spam Against the legal background detailed in the foregoing paragraphs, the Garante is providing the necessary general guidance below to take account of some new spam types and mechanisms that are currently not regulated explicitly by law. This is aimed partly to prevent the huge potential of the Internet and IT in general from allowing, in factual terms, the blanket and/or illegitimate use of personal data.
Clause 6.1 Social Spam	The so-called social spam consists in several activities that allow a spammer to send messages and links via online social networks. This is part of the bigger issue of users´ making use of their personal data recklessly and inadvertently on social networks – which is compounded if "open" user profiles are involved. This situation lends itself to marketing activities and/or other processing operations concerning personal data that are performed for marketing and profiling purposes by third parties, which may be commercial partners of the SNS companies and/or take advantage of the factual availability of such data on the Internet. Furthermore, SNS being social networks of real individuals, spammers can target the contact lists of certain users to enhance the viral potential of their messages. The Garante would like to recall in this regard that the circumstance whereby personal data (such as phone numbers or email addresses) can be retrieved easily on the Internet does not allow using such data to send automated marketing messages without the recipients´ consent. Any marketing message sent to SNS users whether in private or via their public notice boards is subject to the provisions of the Code – in particular to Sections 3, 11, 13, 23 and 130 thereof. The same applies to marketing messages that are sent via increasingly widespread services or tools such as Skype, WhatsApp, Viber, Messanger, etc. Here one should be mindful of the spam proliferation risk, since these services/tools may entail the sharing of all the personal data on one´s smartphone or tablet (addresses, contacts, text messages, browsing data) – which is actually referred to in the respective terms of service – or else may allow the service provider to access the contact lists and/or the address book on one´s mobile phone in order to retrieve or store such personal data. The risk of receiving spam, in particular "targeted spam", based on user profiles might be increased because of the preference shown by the providers of such platforms towards simplified privacy policies that allow merging profiles from different services on a given platform and therefore enable increasingly detailed information to be gathered on users – who may thus receive customized messages depending on their interests and preferences as retrieved from multiple applications. This practice may, on the one hand, facilitate producer-to-consumer relations because it can reduce marketing costs for the former and product search costs for the latter; on the other hand, it may also reduce the recipient´s freedom to make use of information society services (on top of receiving spam) since he/she is being profiled irrespective of his/her consent. Having said that, one should point out that messages sent for exclusively personal purposes remain fully lawful; however, one may also highlight cases in need of clarification from a regulatory standpoint. One such case is where the user receives a marketing message relating to a specific product or service from a company that obtained the user´s personal data from the user´s profile on a SN – irrespective of whether the message is sent privately, to the user´s notice board

or to the email account specified on the user´s SN profile.

Another such case is where the user is a "fan" of a given company or has joined a "group" of followers of a given brand, personality, product or service – i.e., the user has decided to "follow" the relevant news, events or comments – and then receives marketing messages related to such brand, product, service or company.

In the former case, the processing shall be considered unlawful unless the sender can show proof of the recipient´s prior, specific, and free consent under the terms of Section 130(1) and (2) of the Code.

In the latter case, marketing messages concerning a given brand, product or service as sent by the company managing the relevant page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the SNS, also based on the information provided, that the recipient did intend in this manner to also signify his/her intention to consent to receiving marketing messages from the given company. Conversely, if the recipient unsubscribes from the group or stops "following" the brand or personality, or objects to further marketing messages, any marketing message sent thereafter will be unlawful and may carry the applicable punishments. This is without prejudice to the option of blocking messages from specific contacts and/or reporting possible spammers that is offered to users by some SNS.

Regarding an user´s "contacts" (i.e. the so-called "friends"), it is often the case that a SNS or a community can access all the phone numbers or email addresses pertaining to that user; marketing messages may only be sent lawfully to such "contacts" or "friends" if a specific (marketing-related) consent statement is obtained beforehand from each of them.