Silvia Dalle Nogare, Attorney
DFA Studio Legale Associato
Senior Associate

Silvia Dalle Nogare is a senior associate of the DFA law firm.
She deals with international trade and business contracts. She also supports companies in the field of new technologies, with particular reference to legal compliance and contracts relating to e-commerce, protection of personal data and company information, provision of digital services. She is an associate and member of the board of directors of Credimpex Italia, as well as a member of ISOC (Internet Society Italy).

Online retail is constantly increasing, tracking technologies have evolved considerably (e.g. mobile device tracking, augmented reality, social networks, data mining, cloud computing) and personal data of the Internet users are extensively used to provide customized products and services or as currency in exchange for services.
A better access for consumers and business to online goods is one of the pillars on the digital single market strategy of the EU Commission: behavioural tracking is often perceived as a threat to privacy, but it may also be a potential competition issue with reference to exchange of competitively sensitive information.
The speech will comment the legal framework concerning online behavioural tracking, and in particular Regulation 679/2016/UE (GDPR), Decree 196/2003 ("Codice Privacy"), e-Privacy Directive (and the related amendment proposal published on January 2017) and the decision of the Italian Data Protection Authority held on May 8th 2014 ("cookie law") in order to share with the participants a set of guidelines for legitimate profiling.

“Dos and don’ts of online retail: personal data protection vs profiling”

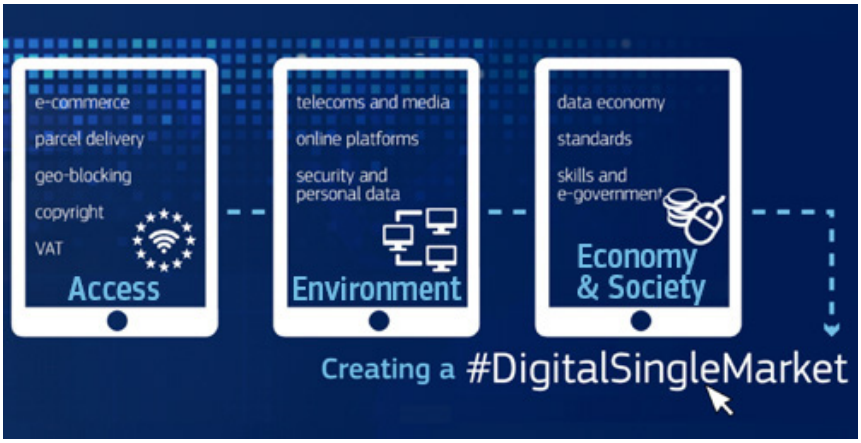
Silvia Dalle Nogare, Attorney
DFA Studio Legale Associato
Senior Associate

Online retail is increasing constantly, profiling technologies (through, for example, mobile devices, augmented reality, social networks, data mining, cloud computing) are evolving rapidly and the Internet users’ personal details are widely used to supply products and personalized services or as “a bargaining chip” for obtaining services.

Better access to online goods for consumers and companies is one of the mainstays of the European Commission’s strategy regarding the digital single market: profiling is often seen as a threat to privacy, but it can also be a potential problem for competition in terms of exchanging strategic information.

The report will comment on the legal framework of reference relating to online profiling, with particular reference to Regulation 679/2016/EU and the provisions laid down by the Italian Data Protection Authority on the subject, with the aim of sharing with the participants the guidelines for lawful and legitimate profiling.

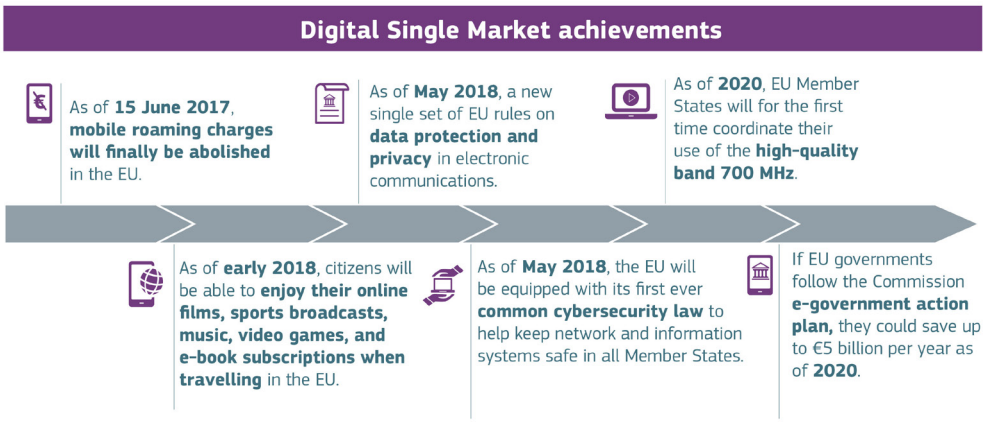
DIGITAL SINGLE MARKET



«A Digital Single Market is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence».
[Source: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market]

The strategy outlined by the European Commission for the Digital Single Market is based on three crucial points:

Access| Environment | Economy & Society



[Source: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market]

In order for digital networks and services to develop correctly, the "digital environment" must include, among other things, trust and safety in the transmitting and processing of personal data.
It would therefore seem that two opposing rights are emerging: one relating to the need to favour the digital development of companies and the protection of free competition, the other relating to user protection (for the most part, "consumers").

WEB MARKETING AND PROFILING

The Treccani dictionary defines Marketing as: "in reference to companies producing fast-moving consumer goods, the set of methods aimed at positioning, with maximum profit, products in a given market by selecting and planning the most opportune product, price, distribution and communication policies, after having identified, through market analyses, the current and potential consumer needs."
Through the Internet, web marketing has developed new sales channels, new assistance modalities, new customer relations modalities: therefore, new business models with which to supply products and services.
Software for managing websites, instruments for indexing websites, tools for creating paid campaigns in the search engine, newsletters, social media: although with different objectives and content, all these instruments process personal data and evaluate surfing behaviour and user habits.
According to the definition in article 4 §4 of **Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data** (for the purposes of brevity "Regulation") «profiling» is "any form of automated personal data processing that consists in the use of such personal data to evaluate determined personal aspects relating to a natural person, in particular for analyzing or foreseeing aspects regarding the professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements of the said natural person."
Online profiling can, therefore, refer to website surfing choices, preferences and interests, demographic data, lifestyles and consumer habits, user geo-localization, and can be carried out explicitly (for example, after filling in an online form) or implicitly (for example, by using cookies).

What, then, are the risks of profiling?
Let's look at a few:

Control of the user by the companies for commercial policy purposes: the new technologies provide a practically instantaneous adaptation of consumer-user habits. Moreover, data processing can be particularly invasive in a person's private sphere and, in the case of incomplete or non-updated data, it can lead to incorrect decisions that significantly affect the person.

Service or price discriminations: through profiling, the goods and services supplier can modify its offer for each consumer, based on selection criteria, such as, gender, age, habits, etc.

Content personalization: the user finds himself/herself accessing only digital content, services and products purposefully selected by digital service suppliers in virtue of information acquired by profiling.

Undoubtedly, the gathering of information, the free circulation of data and online market analysis are now absolutely necessary activities for companies, but it is also true that user profiling should occur in respect of the rights and freedoms of the individual.
Through an analysis of European and Italian legislation on personal data processing and online profiling, we can draw up the guidelines for balancing the interests (often opposing) between online profiling and personal data protection.

THE EUROPEAN REGULATORY FRAMEWORK

The European Union's Charter of Fundamental Rights recognizes the **right to personal data protection** as a fundamental right within the field of European Union law.
The right to personal data protection does not, however, appear as an absolute prerogative but is to be considered in the light of its social function, therefore allowing limitations, if these same limitations are foreseen by the law, should they respect the essential content of the rights and freedom of the individual and, in respect of the principle of proportionality, should they be necessary and effectively respond to the European Union's purposes of general interest or the need to protect the rights and freedom of others.
The current economic and social context in which Italian and international companies are now finding themselves having to operate is, without doubt, characterized by rapid technological evolution and a correlated increase in personal data trans-border flows: «this evolution requires a strong and more coherent framework in relation to data protection in the Union, backed by effective enforcement measures, given the importance of creating the trust that will allow the digital economy to develop across the internal market» (see Recital 7 of the Regulation).
The Regulation is part of the foretold "effective enforcement measures" and, to be more precise, comes within the package of personal data protection reforms launched by the European Commission to adapt the regulation to the changing technological context and global market dynamics.
A fundamental principle of the Regulation and a new element compared to the current regulatory context is «accountability», or rather, the Data Controller's responsibility which is, at the same time, (i) obligation of compliance and (ii) burden of proof of the correct

adoption of the appropriate technical and organizational measures.

How should personal data be processed? Article 5 of the Regulation lists principles like «limitation of purposes», «limitation of preservation», «minimization of data», «data integrity and confidentiality».
When is processing lawful? Article 6 of the Regulation indicates the consent of the Data Subject and the need to execute a contract in which the Data Subject is part, among the conditions of lawfulness.

I will now begin to draw up the guidelines, starting from the concepts of:

limitation of purposes

the data are processed for determined, explicit and legitimate purposes, and are subsequently processed compatibly with those purposes

→ **limitation of preservation**

minimization of data

the data are appropriate, pertinent and limited to pursuing the purposes

integrity and confidentiality

the data are processed in such a way as to guarantee adequate security of the personal data, including protection, by means of appropriate technical and organizational measures, from unauthorized or unlawful processing and from loss, destruction or accidental damage

processing based on the **consent** of the Data Subject or necessary for executing a **contract**.

As a condition of processing lawfulness," consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the Data Subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the Data Subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided." (see Recital 32 of the Regulation).

Continuing with the guidelines, it should be specified that:

consent must be **free, informed, explicit**

since it is free, consent can be **revoked** at any moment

the **statement** that the Data Subject gives must be presented in such a way as to be clearly distinguishable from other parts of the contract or document, comprehensible and easily accessible, using simple and clear language

in order that consent is free, informed, explicit, the Data Controller must provide **information** about processing that is concise, transparent, intelligible and easily accessible using simple and clear language, in writing or using other means

to fulfil the Data Controller's information responsibility, corresponding to the **Data Subject's** cognitive, control and data management **rights.**

Consent and the right to information are also foreseen for **electronic communications** pursuant to Directive 2002/58/EC (on 10th January 2017, the European Commission proposed an amendment to this directive. At the time of drafting this report, the proposal foresaw harmonizing the regulations, an extension of the application field to include electronic communications relating to the supply and use of electronic communication services and to information relating to the end-users' terminal equipment, further protection such as data anonymization, the simplification of some fulfilments, such as consent to use cookies).

Therefore, the Data Controller's duty to inform is still at the core of the privacy regulation, even in reference to new technologies: it is clear that, if the Data Subject has the right to check the ways in which his/her own data are being processed, he/she must receive the appropriate and updated information on the purposes, tools, data storage, subjects to whom the data are being transmitted.

WHAT INFORMATION MUST THE DATA CONTROLLER PROVIDE?
[articles13-14 of the Regulation]

Information to be provided where personal data are collected from the Data Subject

• identity and contact details of the Controller and, where applicable, of the Controller's representative;
• contact details of the Data Protection Officer, where applicable;
• purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
• legitimate interests pursued by the Controller of the third party, where applicable;
• recipients or categories of recipients of the personal data, if any;
• where applicable, the Data Controller's intention to transfer personal data to a third country or international organization;
in addition, at the time when the personal data are obtained
• period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
• existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
• where the processing is based on consent, the existence of right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
• right to lodge a complaint with a supervisory authority;
• if the provision of personal data is a legal or contractual requirement, or if the Data Subject is obliged to provide the personal data as well as the possible consequences of failure to provide such data;
• **existence of an automated decision-making process, 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.**

Information to be provided where personal data have not been obtained from the Data Subject

• identity and contact details of the Controller and, where applicable, of the Controller's representative;
• contact details of the Data Protection Officer, where applicable;
• purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
• categories of the personal data;
• recipients or categories of recipients of the personal data, if any;
• where applicable, the Data Controller's intention to transfer personal data to a third country or international organization;
• period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
• legitimate interest pursued by the Controller of by a third party, where applicable,
• existence of the right to request from the Controller access to and rectification or erasure of personal data or restriction of processing concerning the Data Subject or to object to processing as well as the right to data portability;
• where the processing is based on consent, the existence of right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
• right to lodge a complaint with a supervisory authority;
• the source from which the personal data originate;
• if the provision of personal data is a legal or contractual requirement, or if the Data Subject is obliged to provide the personal data as well as the possible consequences of failure to provide such data;
• **existence of an automated decision-making process, 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.**

Returning to profiling, the Regulation explicitly indicates that the Data Subject has the right "not to be subject to a decision, which can include a measure, that evaluates personal aspects relating to him/her, that is purely based on automated processing and that produces legal effects concerning him/her or similarly significantly affects his/her person, such as the automatic refusal of an online credit application or e-recruiting practices without human intervention" (see Recital 71 and article 22 of the Regulation).
Profiling is, however, allowed, in line with the above outline, where (i) it is necessary for the execution of a contract or (ii) it is based on the Data Subject's explicit consent.
Moreover, the Data Controller is required to use appropriate mathematical or statistical procedures for profiling and to adopt adequate technical and organizational measures in order to «ensure secure personal data processing in a manner that takes account of the potential risks involved for the interests and rights of the Data Subject and that prevents, among other things, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect» (see Recital 71 of the Regulation).
The use of new technologies appears to be in the same character as a general factor that should induce the Data Controller to examine the threats and evaluate the risks, bearing in mind the nature, application field, context and purposes of the processing, as well as risk sources. Article 35 of the Regulation prescribes the Data Controller's obligation to carry out an impact assessment (Data Protection Impact Assessment, hereinafter abbreviated to "DPIA") which, although not formally defined, is essentially a procedure aimed at describing the processing types, evaluating the necessity and proportionality, assessing the risk to the rights and freedoms of the Data Subjects and managing said risk by defining adequate measures to ensure personal data protection and demonstrate conformity to the Regulation.
If, on the one hand, the DPIA draws up, albeit minimal, guidelines that the Data Controller must follow depending on the nature, object, context and purposes of the processing, thereby constructing a risk analysis and risk assessment procedure that refers to the rights and freedoms of the Data Subjects, on the other, the DPIA is documental proof of compliance to the laws that the Data Controller can provide to the competent authorities during an inspection.
The DPIA is not merely a mandatory fulfilment. The Data Controller must perform it as a preventive measure at processing onset, since processing can be a high risk for the rights and freedoms of natural persons.
The use of new technologies, as previously mentioned, is a general application factor of the fulfilment in question. Secondly, the Data Controller must proceed to analyzing processing on the basis of its nature, object, context and purposes and determine whether the risk (if any) is high in relation to the rights and freedoms of natural persons.
The DPIA is particularly required in the presence of a **systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling**, and on which decisions that produce legal effects or similarly significantly affect the afore-mentioned natural persons are based.
Automated decision-making processes, even on account of the fact that they do not allow the Data Subject to intervene, can have discriminatory effects in relation to race, ethnic group, religion, political opinion, the Data Subject's state of health and lead to immaterial damages, like the loss of control over the data, limitation of rights, discriminations, damage to reputation, loss of privacy, identity theft or misuse, as well as material damages, such as economic and financial losses, unauthorized decoding, data destruction, loss or modification.

To add to the guidelines drawn up so far, besides verifying processing conformity to the general principles, ascertaining that conditions of lawfulness exist, providing clear, adequate and complete information and obtaining the consent of the Data Subject,

the Data Controller must proceed to the **impact assessment** foreseen for personal data protection.

What are the «adequate technical and organizational measures»?
The Regulation lists (in a non exhaustive manner) measures such as the pseudonymization and coding of personal data; capacity to permanently ensure the confidentiality, integrity, availability and resilience of data processing systems and services; capacity to punctually reset personal data availability and access in case of physical or technical accident; procedures for testing, checking and regularly evaluating the effectiveness of the technical and organizational measures in order to guarantee secure data processing.
The decision to adopt technical and organizational measures falls to the Data Controller, as a consequence of the principle of accountability: in evaluating the adequate level of security, the Data Controller must take into account the processing risks, especially those deriving from the destruction, loss, modification, unauthorized divulgation or access, both accidental and illegal, of transmitted, stored or, in any case, processed personal data.

THE ITALIAN DATA PROTECTION AUTHORITY PROVISIONS FOR ONLINE PROFILING AND COOKIES

With the **Provision of 8th May 2014**, the Italian Data Protection Authority identified simplified arrangements to provide information and obtain consent regarding cookies:

(i) cookies are defined as small text files that are sent to the user's terminal equipment by visited websites where they are stored to then be re-transmitted to the websites on the user's subsequent visits to those websites. When surfing a web site, the user may receive cookies from other websites or web servers, on which some elements may reside (like, for ex ample, images, maps, sound files, links to other web pages on different domains) located on the site that is being visited.

(ii) depending on their purposes, cookies are subdivided into "technical" and "profiling", and, depending on the subject that installs them, they are identified as "publishers" or "third parties."

I will use the summary table proposed by the Italian Data Protection Authority to examine the fulfilments in relation to each of the above-mentioned cookie types:

With the Provision of 19th March 2015, the Italian Data Protection Authority published data processing guidelines for online profiling:

(I) the general picture highlights that, in the majority of cases, the data collected are used for profiling purposes and for instru mental use in relation to the goods or services offer in question;

(II) users can be distinguished between "authenticated users" and "unauthenticated users";

(III) the Data Controller must therefore provide information, request the consent of the Data Subjects for profiling purposes, consent to the correct exercising of the Data Subject's rights, store the data for a period of time that is suitable for the pur poses of the data collection.

information easily accessible on all devices and applications, formulated clearly, completely and exhaus-tively, updated, rendered according to «multilayer» formats (I and II levels)

II level	any previous versions of the information could be archived together with indications on the specific risks that may arise for the Data Subject from using the services and other suitable indications to give a more effective exercising of the users' acknowledged rights

consent	free, acquired before processing occurs, referable to processing that pursues explicit and determined purposes, informed and documented in writing, diversified in relation to the type of user in question
unauthenticated user	on entering the site, a suitable information area which (i) indicates the data processing activity for profiling purposes, (ii) provides links to information and to another specific area where it is possible to refuse consent to profiling, or, if applicable, to select, in an absolutely analytical manner, profiling functionalities and modalities, (iii) indicates that profiling consent is required in order to continue surfing.

data retention policy in compliance with the principle of purpose

CONCLUSIONS

Going back to the text in Regulation Recitals 6 and 7, «technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of personal data protection.»
In order to create a climate of trust that would allow the digital economy to develop throughout the internal market, it is necessary that natural persons (both users and consumers) maintain control of their own data and are placed in the condition of being aware of processing modalities and purposes.

I will conclude by quoting an extract from the essay by prof. Stefano Rodotà, The world in Internet: rights and restrictions:
«the change was accepted when it was realized that the traditional notion of privacy was no longer able to include such a profoundly modified dimension. Its original construction reproduces the model of private property that excludes others, within which nobody can lawfully penetrate. The electronic revolution has transformed the very notion of private sphere, which had more and more intensely become a place of exchange, of personal data sharing, of information, the circulation of which no longer only regarded outgoing information but also incoming information with which others were invading that sphere in ways that were increasingly widespread and unwanted, and thus continually modify it.
The shift from the original notion of privacy to the principle of data protection also corresponds to a profound change in the modality of private sphere invasion. Nowadays, violation opportunities accompany almost every moment of our daily lives: we give information, we leave traces when we are supplied with goods and services, when we search for information, when we move in real or virtual space. Our social representation is increasingly entrusted to information scattered in a multitude of databases and to profiles that are constructed on this base and the simulations that they allow. Having become disembodied entities, people are in increasing need of protection for their "electronic body".»