The Public Administration and the Citizens Privacy Protection.
A Comparison Between European Union and Japan

Giacomo Mannocci*

Abstract

Cybersecurity and privacy protection are strategic objectives to ensure free trade and economic freedom in a global society. Precisely for this reason, recently, the European Union and Japan have changed their legislation on the protection of personal data, strengthening the powers of control and regulation by public bodies. Ensuring citizens of the proliferation of data on the internet has become a necessity. This is demonstrated by the recent scandals involving Facebook and Cambridge Analytica.

I. Introduction

In the past years privacy protection and information security have become topical: the Privacy Right, meant as the right to protect the inner life from various interferences, is strictly linked to the tutelage of a person dignity.

The emergence of social networks and internet development created a new problem: the 'unauthorized profiling' of personal data. The services offered on internet, inevitably require the acquisition of information regarding the personal sphere: every day, a huge quantity of personal data, imagines and inclinations are put online. So, the data became exchange goods always more exposed to continuous collection and monitoring, often in occult ways. The 'Over The Top' (that is a label to indicate the big internet monopolists which declared a commercial interest) collect and register personal data in huge servers; these data are provided by the users for many different reasons. In this way such societies realize the most sophisticated forms of behavioral advertisement, becoming brokers, even more exclusive, between producers and consumers, they orientate choices and often knowledge, accumulate major wealth and negotiate as pair with governments. Governments and police authorities themselves collect and treat data put on the net by the users for legitimate security reasons. The will to prevent terroristic threats immeasurably multiplied the collection and classification of information and data regarding citizens lives and behaviors.

In this social contest it becomes even more necessary to find a balance

* PhD in Constitutional Law, University of Genoa.

between the need to protect people privacy (and so dignity), by ensuring national and international security from terroristic threats and, at the same time, the priority of supporting free circulation of data and free competition between economical operators.

The privacy regulation is in continuous evolution because it has 'to run after' and 'to answer' to new information and technological discoveries. For this reason, it is interesting to analyze, in a comparative way, how European Union and Japan have recently modified their legislation about personal data protection. On 25 May 2018 came into force the new Privacy European Regulation[1] which replaces the one of 1996.[2] The previous year, on 30 May 2017 in Japan, came into force the new privacy laws which replaced quite totally those of 2003 and took into consideration the technologic evolution of the last decade.

In the current contribution, the European and the Japan Regulation will be seen by a particular perspective: it will be examined how Public Administration protect privacy of its citizens and most of all how it guarantee their rights against the intrusiveness of economic operators. The recent scandal that involved Facebook is an example: the well-known social network yielded millions data of its users to the society called Cambridge Analytica,[3] which in turn has used them to influence voter choices in many electoral competitions. So the active role of Public Institutions becomes fundamental to avoid not only the privacy violation but also the market alteration due to an unfair competition.

II. The Privacy Protection in Japan

In Japan, the privacy protection of personal data has an implicit foundation in the Art 13 of the Constitution, according to which

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] The GDPR supersedes EC Directive 46/95 currently in force, implemented in Italy through the Legislative Decree 196/03 (Data Protection Law). The Legislative Decree on the harmonization of the national legislation with the provisions of the GDPR (the 'Decree 101/2018'), which amends Legislative Decree 196/2003 (the 'Privacy Code') was published on 4 September 2018 and it is came into force on 19 September 2018. The new regulatory framework for the protection of personal data is therefore made up of the GDPR, the amended Privacy Code, Decree 101, but also Law 11 January 2018 no 5 (telemarketing reform), as well as Legislative Decree 18 May 2018 no 51 (regarding the protection of personal data in processing for the purposes of prevention, investigation, verification and prosecution of crimes or execution of criminal sanctions).

[3] For a more detailed historical reconstruction, see Information Commisioner's Office, *Investigation into the use of data analytics in political campaigns*, 2018, available at https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf (last visited 15 November 2018).

> 'All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs'.[4]

Japan's Act on Protection of Personal Information (Act no 57 of 2003, known by the acronym APPI), one of Asia's oldest data protection laws, was originally created in 2003, and came into effect in 2005.[5] Over the following decade, developments in information technology and the globalization of data have had the effect of aging the APPI and shifting it out of line with internationally accepted standards. On 24 June 2014, the Japanese Government published the Policy Outline of the Institutional Revision for Use of Personal Data.[6] Changes to the APPI were passed by the Diet in September 2015. Some provisions, mainly those establishing and governing the Personal Information Protection Commission (PPC) (1 January 2016), are in force, and the remaining provisions are taking effect on 30 May 2017.[7]

As groundwork for the enforcement of the new APPI the Government has prepared the amended basic policy of the protection of personal information as decided by the Japanese Cabinet on 28 October 2016, the new cabinet order[8] the enforcement rules of the Amended APPI as published on 5 October 2016 and the guidelines[9] of the Amended APPI. The guidelines of the Amended APPI, which were published on 30 November 2016, contain guidance regarding: general rules, offshore transfer of personal data, book-keeping and verification obligations when transferring personal data to a third party and big data processing. These foundational policies, rules and guidelines will become effective upon the enforcement date of the Amended APPI.

The 2015 law is deeply innovative compared with the past one and it guarantee more protection to citizens, in fact the limit which scheduled the rule applicability only to the economic operators which had personal information database containing details of more than five thousand persons on any day in

[4] For a more detailed analysis and discussion on Japanese Constitution, see S. Matsui, *The Constitution of Japan: A Contextual Analysis* (London: Bloomsbury Publishing Plc, 2010). For a more detailed explanation and interpretation of the Human rights in Japan, see T. Kuramochi, 'The Protection of Human Rights and the Role of Constitutional Judicial Review in Japan' 26 *King's Law Journal*, 252-265.

[5] Act no 57 of 30 May 2003, enacted on 30 May 2003 except for Chapters 4 to 6 and Arts 2 to 6 of the Supplementary Provisions; completely enacted on 1 April 2005 and amended by Act no 49 of 2009 and Act no 65 of 2015.

[6] Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, *Policy Outline of the Institutional Revision for Utilization of Personal Data,* 2014, available at https://tinyurl.com/y9to4who (last visited 15 November 2018)

[7] The English translation of the amended Act on the Protection of Personal Information is available at https://tinyurl.com/ydaphnxj (last visited 15 November 2018).

[8] https://tinyurl.com/y9ozgjot (last visited 15 November 2018).

[9] https://tinyurl.com/yaelm62x (last visited 15 November 2018).

the past six months[10] has been canceled; then it is granted to a single independent administrative authority the role to write the privacy guidelines, while until 2015 many Ministry or independent agencies were granted to issue guidelines about their proper competences. Approximately forty guidelines regarding personal information protection have been issued by government agencies including the Ministry of Health, Labour and Welfare,[11] the Japan Financial Services Agency[12] and the Ministry of Economy, Trade and Industry.[13]

The law hasn't limited itself only to establish the new field of competence of publics organisms, but it also influenced deeply the personal data notions to guarantee them a more effective protection. Among the most significant innovations of this law, it is important to remember the widening of the concept of personal data to comprehend the 'individual identification code' (Art 2 para 2), the introduction of the 'Special care-required personal information' concept (Art 2 para 3) to indicate the valid data to gather information about health conditions, racial origins, crime committed and so on and the creation of the 'Anonymously processed information' category (Art 2 para 10) to indicate the revision and the annexation of data without going up again to single personal data.

It is interesting to observe that the new law, according to what established in 2003, lays down the duties of the National Government and of local administrations as regards the citizens' privacy protection. First, it established that

> 'The central government shall have the responsibilities for comprehensively developing and implementing necessary measures to ensure the proper handling of personal information' (Art 2)

and then it clearly state that

> 'The government shall, considering the nature and utilization method of personal information, take necessary legislative and other action so as to be able to take discreet action for protecting personal information that especially requires ensuring the strict implementation of its proper handling in order to seek enhanced protection of an individual's rights and interests, and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning

[10] Art 2 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003).

[11] The Guidelines on Protection of Personal Information in the Employment Management (Announcement no 357 of 14 May 2012 by the Ministry of Health, Labour and Welfare).

[12] The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement no 63 of 20 November 2009 by the Financial Services Agency).

[13] The Guidelines Targeting Medical and Nursing-Care Sectors Pertaining to the Act on the Protection of Personal Information (Announcement in April 2017 by the PPC and the Ministry of Health, Labour and Welfare).

> personal information through fostering cooperation with an international organization and other international framework' (Art 4).

The law also specifies the role and the functions of local authorities in the personal data management. Thus, Arts 11-13 establish that each local government shall:

- based on the nature of personal information it retains, the purpose of retaining the personal information, and so on, strive to take necessary action so as to ensure the proper handling of the retained personal information (Art 11 para 1);
- in response to the characteristics and business contents of a local incorporated administrative agency that it has established, strive to take necessary action so as to ensure the proper handling of personal information that the agency retains (Art 11 para 2);
- in order to ensure the proper handling of personal information, strive to take necessary action to support a business operator and a resident in a local area (Art 12);
- in order for a complaint caused between a business operator and a principal about the handling of personal information to be dealt with appropriately and promptly, strive to mediate dealing with the complaint and take other necessary action (Art 13).

Finally, it is establishes as a general standard that central and local governments cooperate with each other in the implementation of measures concerning the protection of personal information (Art 14).

One has to observe that the new law has strengthened the Prime Minister's role because as until 2017 single Ministries issued their proper guidelines. It now belongs to Government as a whole to establish

> 'a basic policy on the protection of personal information in order to seek to comprehensively and integrally promote measures concerning the protection of personal information' (Art 7).

Moreover, it is the Cabinet to establish agreements with other Nations about data and information circulation, as well as to give directions and support to local administrations. By the same token, it is a Prime Minister's duty to propose the adoption of new technical rules, to nominate the President and the members of the Personal Information Protection Commission.

This Commission is the other news of the 2015 law because it will have a real propulsive role for the privacy theme and it will represent the reference point both for Government, local authorities and most of all for economic operators. Its functions are very wide, in fact the Commission:

- provides guidance and advices, requests reports, conducts on-site inspections, offers a recommendation and makes orders to governmental institutions and

business operators who handle Specific Personal Information, depending on the issue;

- mediates the complaints with regard to the handling of Specific Personal Information;

- announces and promotes the importance of personal information protection, as well as proper and effective use of personal information;

- promotes cooperation with data protection authorities in foreign states;

- acridities private organizations, which process complaints on business operators handling personal information and provide information to them.

The Commission is composed by a chairperson and eight Commission members, appointed by the Prime Minister with the consent of both Houses of the Diet. The term of offices of the chairperson and the Commission members is five years. The chairperson and Commission members exercise their authorities independently.

While the President and the Vice-President can be chosen freely, the other six members are chosen based on specific competences acquired in their academic or working field. The Japanese Legislator's aim was to permit that the Commission would have those specific competences necessary to examine privacy problems with a multidisciplinary view. In fact it comprehend:

- A person who has knowledge and experience in the protection and in appropriate and effective use of personal information

- A person who has knowledge and experience in the protection of consumers

- A person who has knowledge and experience in information processing technology

- A person who has knowledge and experience in administrative fields used in specific personal information

- A person who has extensive knowledge and wide experience in matters relating to the practices of private enterprises

- A person recommended by six federations composed of governors, mayors and presidents of the local councils.

III. The New European Privacy Regulation

In the same period in which Japanese Government started to reform its privacy regulations, European Union completely updated its own, which dated back to 1996.

Since the mid-1990s, EU policymakers have adopted a series of data protection rules that quickly became the de facto global standards for most countries except for a few holdouts like China, Russia, Japan and the United States.

Before briefly examining the new EU regulation, one has to highlight a fundamental difference between the European and the Japanese one. In fact, in Japan the 2015 law not only regulates the basic aspects of the personal data

management, but it also clearly indicates the competences of the independent administrational Agency which have to supervise the respect of the rules. By contrast, in Europe the European Data Protection Supervisor will still have to be regulated by the 2001 Regulation and not by the General Data Protection Regulation of 2016. This will require to harmonize the Supervisor figure in the context of the new Regulation. The problem is well known, in fact the European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001[14] and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. Both the ePrivacy[15] and Regulation 45/2001 replacement texts should be adopted in time to become applicable at the same time as the GDPR. With this comprehensive reform, the EU will have a modern framework for privacy and data protection.

In light of the above, it is now necessary to analyze the most innovative aspects of the new Personal Information Protection Regulation.

After four years of preparation and debate the General Data Protection Regulation (acronym GDPR)[16] was finally approved by the EU Parliament on 14 April 2016.

The EU General Data Protection Regulation replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and to empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Over the last 25 years, technology transformed lives of European citizen in ways nobody could have imagined, thereby requiring a review of the old rules. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly

[14] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. For a legal analysis of this regulation, see K. Runeberg, Balancing the Right to Data Protection and the Right of Access to Documents. A Study of the Conflicts Between Regulation 45/2001 and Regulation 1049/2001, Faculty of Law, Lund University, 2018, avalaible at https://tinyurl.com/y9q2pq4v (last visited 15 November 2018).

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). For more details, see L.F. Asscher and S. A. Hoogcarspel, *Regulating Spam. A European perspective after the adoption of the e-Privacy Directive* (Berlin: Springer, 2006).

[16] There is a considerable body of scientific literature on the GDPR. In particolar, see P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Berlin: Springer, 2017); C. Kuner, L.A.Bygrave and C. Docksey, *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2018); G. Voss and K. H. Woodcock, *Navigating EU Privacy and Data Protection Laws* (Chicago: American Bar Association, 2016); Paul Lambert, *Understanding the New European Data Protection Rules* (Boca Raton: Auerbach Publications, 2017).

data-driven world that is vastly different from the time in which the 1995 directive was established.

The GDPR is now recognized as law across the EU and Member States have two years to ensure that it is fully operational in their countries by May 2018: they must implement the Data Protection Directive for the police and justice sectors into national legislation. It will be applicable as of 25 May 2018.

It will be applied to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Another legislative change concerns the conditions for the consent from the citizens. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

The GDPR provides the following rights for individuals:

1. The right to be informed (It encompasses an obligation to provide '*fair processing information*', typically through a privacy notice. It emphasizes the need for transparency over how you use personal data. Furthermore that is the right to be informed of a data protection breach)

2. The right of access (everyone have the right to obtain confirmation that their data is being processed; and access to their personal data; and other supplementary information)

3. The right to rectification

4. The right to erasure (this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing)

5. The right to restrict processing (when processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future)

6. The right to data portability (The right to data portability allows individuals to obtain and to reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily in a safe and secure way, without hindrance to usability)

7. The right to object, namely right to object to:

a) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
b) direct marketing (including profiling);

c) processing for purposes of scientific/historical research and statistics

8. Rights in relation to automated decision-making and profiling because the new law provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

These rights are guaranteed with the provision of precise obligations for the controller. Financial penalties are also provided. The controller must not refuse to give effect to the rights of a data subject unless the controller cannot identify the data subject. The controller must use all reasonable efforts to verify the identity of data subjects. Where the controller has reasonable doubts as to the identity of the data subject, the controller may request the provision of additional information necessary to confirm the identity of the data subject, but is not required to do so.

These are very briefly the novelties concerning the rights protected by the Regulation: it is important to underline that such instrument is extremely complex and detailed and for this reason it is not possible to summarize it in a few pages. But here, it will be added the Public Administrations duties of the single members Nations to make effective the right above quoted. The European Legislator, in fact, established that the same duties which are imposed on the economic operators also apply to Public Administrations. Those are:

1. Data Protection Officer. The GDPR introduces a duty to appoint a Data Protection Officer (DPO) for a public authority, or for carrying out certain types of processing activities (Art 37). DPOs give assistance to monitor internal compliance, to inform and to advise on your data protection obligations, it provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and reported to the highest management level. A DPO can be an existing employee or externally appointed. In some cases several organizations can appoint a single DPO among them. DPOs can help to demonstrate compliance and are part of the enhanced focus on accountability.

2. Records of processing activities. Art 30 of the GDPR obliges companies and Public Administration to maintain 'records of processing activities'. The processing records serve to ensure transparency with regard to processing personal data and to provide legal protection for the company. It can support the company's data protection officer, as well as the supervisory authority in carrying out their tasks. In accordance with Art 30, para 4, of the GDPR, the controller or the processor shall make the record available to the supervisory authority on request. The processing records also serve as verification, so the company can prove to the supervisory authority that the requirements of the GDPR were fulfilled by the controller.

Part of the general duty of the controller is the cooperation with the supervisory authority, on request, in the performance of its tasks (Art 31 of the GDPR).

3. Data protection impact assessment. (Art 35) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller is responsible for carrying-out a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment is taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. When a data-protection impact assessment indicates that processing operations involve a high risk, which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority takes place prior to the processing.

IV. The Data Transfer Between Japan and EU

Finally, we are going to examine the relationship between EU and Japan. On July 2017, the European Commission and the Japanese Government published a joint statement on international transfers of personal data.[17] The statement mentions that the EU and Japan will continue their cooperation and aim by early 2018 to recognize each other as having adequate levels of personal data protection. If this does indeed occur, it would mean there would be compliant transfers of personal data between the EU and Japan without the need for instruments such as standard contractual clauses, binding corporate rules or privacy certifications.

How explained before, from the technical point of view, is the Japanese PPC that has to engage in relationships with foreign Authorities which attend to regulation and transfer of personal information. It is for this reason that since its assignment in 2016, the Commission has started a worthwhile dialogue with the European Commission and with the single EU Nations to manage the personal information transfer and utilization between Japan and Europe. There is, in fact, the need to harmonize the Community Regulation and the Japanese one to make commercial exchange easier that is of fundamental importance for both.

To establish a fundamental framework for mutual and smooth transfers of personal data between Japan and the EU, in June 2017, the PPC proposed the following criteria to be set forth as amendments to the PPC Rules for designating a foreign country (which is an alternative measure to obtaining the data subject's consent for a cross-border transfer of personal data from Japan to a foreign country under Art 24 of the APPI):

- there are statutory provisions or codes equivalent to those relating to the

[17] The cross-border flows of personal data are governed by Chapter V of GDPR (arts 43-50).

obligations of personal information handling business operators defined under the APPI, and the policies, procedures and systems to enforce compliance with these rules can be recognized;

- there is an independent personal data protection authority, and the authority has ensured the necessary enforcement policies, procedures and systems;

- the necessity for a foreign country designation can be recognized as in Japan's national interests.

In February 2018, the Japanese PPC reported on a plan to establish additional Guidelines being applicable to personal data transferred from the EU to process it in Japan under the mutual adequacy findings. The PPC recognizes the following major differences between the APPI and the GDPR, and plans to reflect them in the additional Guidelines:

- Scope of the data subject's rights on the retained personal data – the data subject's rights requesting disclosure, correction, suspension of usage, etc. shall be given to any personal data transferred from the EU regardless of the duration of the data retention period;

- Sensitive data – personal data regarding sex life, sexual orientation, and labor union membership transferred from the EU shall be treated as equivalent to 'special care-required personal information' under the APPI;

- Anonymized data – 'anonymization' of personal data transferred from the EU shall mean no one can re-identify a specific individual data subject by discarding decryption keys (different from 'pseudonymization'). Such data is treated as anonymously processed information under the APPI.[18]

At the moment, a comprehensive agreement is lacking even, though it is likely to be reached in a few months because it is a cardinal matter fundamental for both.

V. Conclusions

Pointing out to the European Legislation and the Japanese one, it can be noticed that the fundamental aim is the same: protect individuals from intrusiveness, sometimes really excessive, of economical operators, most of all operating in the Net. If it is right that all laws are perfectible, this statement is more pregnant when speaking about privacy and informatics security because technology necessary brings to face aspects until that moment have been unthinkable. The challenge is not only to have Legislation in the forefront, but also to have a Public Administration able to utilize tools that new rules grant. For example, the European Regulation gave two years (2016-18) to State members to bring in line their administrational structures according to Community requirements.

[18] Y. Watanabe, 'Japan EU Data Transfers - Mutual adequacy findings under APPI and GDPR' (2018), available at https://tinyurl.com/y8wzmxbg (last visited 15 November 2018).

Now then, in some cases, like in Italy, time passed uselessly. Actually, the Italian Government approved the measures to actuate the new Community duties only in March 2018, two months before the direct enforceability of new dispositions. This is creating many problems because many administrations, particularly Cities, are not able to front new requirements. There is also a lack of specific formation for public employees, who will be called to really actuate the Community Regulation. We are still in 'work in progress'.