ITALY

MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION
Inter-ministerial Committee for Human Rights
Comitato Interministeriale per i Diritti Umani

ITALY'S CONTRIBUTION, PURSUANT TO UN HUMAN RIGHTS COUNCIL RESOLUTION 34/7 "THE RIGHT TO PRIVACY IN THE DIGITAL AGE"

APRIL 2018

ITALY'S CONTRIBUTION

To the attention of:
privacyreport@ohchr.org
registry@ohchr.org

Following your query, we are in a position to provide the following information for your use only:

Telemarketing

1. In the Italian context, the processing of personal data for commercial and advertising purposes is of specific attention for citizens, given the greater awareness of consumers about the value of their own data. In recent decades we have witnessed the convergence of the advertisement campaigns, thanks to the pervasiveness of services based on data request and profiling. As a way of examples, mention may be made of new tools such as social networks, instant messaging services, the most invasive apps, which coexist with more traditional practices such as coupon signing, discount cards, and fidelity cards.

2. Despite the multiplication of channels through which to offer products, in Italy telemarketing by telephone still remains one of the sales and promotion channels most preferred by commercial operators. Although it may prove to be a very useful tool for the consumer (and competition) especially in the telecommunications and utilities sector, unwanted advertising in-bound calls are perceived by citizens by annoyance and sometimes exasperation.

3. The ease of access to the databases set up to create telephone directories by external companies that do telemarketing without the interested subscribers were aware of it has led the Italian legislator to intervene.

4. Article 20-bis of Act No. 166/2009 introduced changes to the processing of data in public telephone directories by commercial operators. Compared to the previous regulatory framework based on the opt in - that allowed to contact by telephone for advertising campaigns only those who had previously given their consent -, the legislator has favoured the opt-out system for which the subscriber can express his/her dissent to receive unwanted advertising calls by registering in a special list called "Public Register of Oppositions".

5. The transition from the legal system of the opt in to opt out was carried out in accordance with Directive 2002/58/CE (Article 13 paragraph 3), containing the provisions on privacy and electronic communications.

6. As a consequence, in Italy a *Robinson list* has been also established by D.P.R. 178/2010, called "Regulation establishing and managing the public register of subscribers who oppose the use of their telephone number for sales or commercial promotions purposes".

7. The aforementioned Decree contains provisions regarding the rights acquired by the members, the technical implementation, management and operation for the subscribers and operators, as well as indications on the conduct of a specific information campaign: The introduction of the opt out represents the fair reconciliation of the interests, with aim at ensuring compliance with privacy legislation in a competitive environment in which the principle of free economic initiative can be fully affirmed. With the new system, the citizen has become more aware of his/her rights, reaching a maturity in which to acquire an active role.

8. It is a solution that balances the rights and duties of the stakeholders without damaging the occupational sector. The adopted legislation, therefore, contributes to boosting the telemarketing market, giving responsibility to all the actors involved. With the introduction of the Public Register of

Oppositions - from 1 February 2011 onwards - clear and effective rules have been established to safeguard the privacy of the citizen and regulate the management of telemarketing.

9. Even if the advertising calls to the reserved numbers, both fixed and mobile, can only be carried out with the consent of the party concerned (with the exception of a few exceptions specified by the Code regarding the protection of personal data and the Provisions of the Privacy Authority), violations of national legislation are to be reported significantly.

10. Many users have raised the problem of lack of clarity and transparency in the practice of acquiring consent under forms and contracts.

11. The consent to the processing of personal data for the purposes of sending advertising materials or direct sales or for carrying out market research or commercial communication are often included in the contracts themselves and their voluntary nature is not perceived by the citizen.

12. It is also burdensome to assert rights when it is provided, sometimes unconsciously, consent to the transfer of their data to third parties, thus effectively losing control. This phenomenon appears to be one of the most felt by citizens, considering that this consent often has almost unlimited duration and value.

13. By Law No. 124/2017, Article 130, para. 3-bis of the protection of personal data Code, has been implemented, by specifically extending the opt out on the treatment of postal addresses present in public telephone directories by telemarketing operators to the on paper.

14. Following a long analysis of all the critical issues emerged after the first significant regulatory measures on wild telemarketing, the legislator returned to intervene by Law No. 5/2018, which extends the possibility of registration in the Public Register of Oppositions to all reserved numbers, meaning all fixed and mobile phones not present in public telephone directories.

15. The new law introduces important changes to protect citizens' privacy. First of all the cancellation of the consent previously given by citizens for advertising purposes when the entry in the Register will become effective. However, it will always be possible to authorize the single commercial subjects to the advertising calls, but in a conscious way.

16. The most significant changes are shown below:

- possibility of registering with the Public Registry of the Oppositions of all telephone numbers, including mobile and fixed phones not included in public telephone directories;
- in parallel with the registration in the Register, cancellation of consent to the processing of personal data for commercial purposes previously conferred by citizens, except for consent granted "in the context of specific contractual relationships in place, or ceased by no more than thirty days, concerning the supply of goods or services, for which the right of revocation is assured with simplified procedures";
- prohibition of the transfer to third parties of the consent to the processing of personal data of the members in the new Register;
- prohibition of using automatic composers to search telephone numbers;
- enhancement of the sanctions, up to the suspension of the activity and the revocation of the license in case of failure to comply with the law by single call centers;
- call center obligation to make calls with identifiable and recallable number, alternatively to use a specific prefix;
- obligation for the call centers to check at the Public Registry of the Oppositions, at least once a month, that the numbers they intend to call for advertising purposes are not entered in the Register.

Surveillance and interception of communications: data retention

17. Respect for privacy and the right to protection of personal data are recognized fundamental rights, so any limitation on the exercise of these rights aimed at ensuring national security, in addition

to being provided for by law, must constitute a necessary measure in a democratic society (legality, necessity, proportionality test).

18. The data retention in Italy is set by the privacy Code in two years for telephone traffic, one year for the online/telematic one, and 30 days for unanswered calls. By the anti-terrorism Decree 2015, it has been amended, imposing until 30 June 2017, the obligation to keep data relating to telephone or telematic traffic, excluding, however, the communication contents held by telecommunication services operators, those relating to traffic, as well as data on unanswered calls, processed temporarily by providers of electronic communications services accessible to the public or by a public communications, telephone or telematic network.

19. At the end of the deadline of 30 June 2017, by European Law 2017, given the high importance of historical data on traffic to investigate and / or prevent the most serious crimes (e.g. for terrorism purposes), the term of conservation of data traffic has been extended to 72 months. With regard to interception, the services to be charged to the communication operators are defined by ministerial decrees implementing the provisions of Art. 96 of the electronic communications code (Legislative Decree No. 259/2003).

Adjustment to the new EU regulatory framework-2018

20. In accordance with EU General Data Protection Regulation (Regulation (EU)679/2016, hereinafter 'GDPR'), directly applicable from next May 25th, the legislator is working on a Bill, which will align the current Data Protection Code (Legislative Decree No. 196/2003, hereinafter 'DPCode') to the new EU regulatory framework.

21. The GDPR has introduced some remarkable changes in the data protection landscape: an increased territorial scope (extra-territorial applicability) of its provisions; strong penalties for breaches of data protection rules; stricter requirements for the use by data controllers of data subject's consent as legal basis for the processing of personal data; strengthened data subjects' rights (including data portability); strengthened responsibility of data controllers (accountability) in respect of data processing, including the duty to provide solutions and to preliminarily assess the impact of the intended processing on individuals' fundamental rights (Data Protection Impact Assessment).

22. The protection of privacy in the electronic communications sector is also under review at a EU level, as Directive 2002/58 (so called e-Privacy Directive) will be updated by a new Regulation, aimed at reinforcing trust and security in the EU Digital Single Market by giving directly applicable rules, taking into account the new players currently active in the e-market besides providing for a stronger protection of privacy in respect of communications content and meta-data.

23. The Italian legislator is also currently working on the implementation of 'Directive (EU) 680/2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'. Such Directive is – together with the GDPR- a main pillar of the EU reform in data protection field.

24. The Italian Data Protection Authority (the 'Garante'), through an opinion dated 22 February 2018 on the Bill implementing Directive 680/2016, signalled some possible amendments to ensure full respect for data protection principles as foreseen by the same Directive and by the EU framework (including the ECJ's case law), in particular concerning data retention periods.

25. With regard to interceptions, *Garante*'s Opinion issued on 2 November 2017 concerning the Bill, which provides for substantial modifications of wiretapping, in particular in respect of transcriptions and use of tapping for precautionary measures and the conditions and requirements for the admissibility of wiretapping by means of computer sensors contained in portable electronic devices. This Opinion provides for specific safeguards aiming at strengthening the preliminary control by the judge on investigative activities.

Encryption and anonymization

26. Encryption and anonymization are crucial elements from a data protection perspective, not by coincidence often indicated by the above *Garante* as important safeguards for ensuring secure data processing, in particular in respect of special categories of data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or concerning a natural person's sex life or sexual orientation: see Article 4.1.d of the DPCode, Articles 4 and 9 of the GDPR, and Articles 3 and 10 of Directive 680/2016). For example, pursuant to Article 6 of the DPCode, sensitive or judicial data that is contained in registers or data banks kept with electronic means must be processed by using encryption techniques, identification codes or any other system such as to make the data temporarily unintelligible also to the entities authorised to access it and allow identification of the data subject only in case of necessity. Article 34 on minimum security measures for processing by electronic means also considers encryption to be ensured in particular in respect of health data.

27. The GDPR also provides for specific norms on encryption such as in Article 6.4.e, 32.1.a, 34.3.a.

28. With regard to the specific challenges raised by anoynimisation, as often recalled by the Authority under reference and by the Article 29 Working Party (the Working Party composed by EU data protection authorities), it is essential for the data controllers to take into account the risk of re-identification in particular when – and always - new technologies render re-identification more and more easy.

29. Encryption as well must be assessed according to the available technologies which may easily decrypt data that in the past was deemed to be safely encrypted. (see Article 29 work on anonymisation, in particular Opinion 05/2014).

30. The Italian DPCode provides for specific norms telephone and electronic communications traffic data's retention by providers (Article 132). This provision underwent several amendments in the last few years. Law No. 167/2017 extended data retention of such traffic to 72 months in view of the need to contrast terrorism. The *Garante* intervened by Note dated 22 December 2016 by which it underlined that the 6 years-term for the retention of all traffic data is in contrast with the EU legal framework and the European Court of Justice case law, which considers bulk collection of data, non proportioned to the investigation needs and the essence of data protection to be unlawful.

31. It is now possible to provide for the obligation to collect data but only for specific objectives, namely the prosecution of serious crimes, only if such obligations are limited in timing in a proportionate manner and concern only the information which is strictly necessary to such aim.

- Technology plays a crucial role in helping promote and protect the right to privacy. The GPDR (as well as many decisions issued at national level by the Garante) gives a big emphasis to privacy by design and privacy by default principles. According to such principles, (see Article 25 of the GDPR) taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, data controllers must implement appropriate technical and organisational measures, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the data protection requirements and protect the rights of data subjects. Moreover, controllers must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. According to

the GDPR approved certification mechanisms may be used as an element to demonstrate compliance with such requirements.

- Biometric data is particularly sensitive as it leads to the unique identification or authentication of the individual. It has the potential to adversely affect and discriminate data subjects and is subject to possible risks of inaccuracy, such false matching. Its processing must therefore be submitted to strict assessment of the necessity and proportionality of the processing, the quality of data, and to rigorous security measures.

- More generally, growing reliance on data-driven technology, more and more linked to profiling and/or automated decisions on individuals must be carefully considered to avoid the risks, amongst others, of: bulk collection of data, use of data for purposes which are not compatible with the original legitimate purpose of the processing, inaccurate or discriminatory conclusions on individuals, lack of valid legal basis for the processing, opacity of the processing (which does not allow the data subject to be aware of the processing of data related to him/her and eventually exercise his/her rights).

- The transnational nature of data processing requires for the provision of common standard at a global level, without which the protection of individuals would not be sufficiently ensured.

32. Law No. 71/2017 introduced the notion of cyberbullying. According to Article 2 any minor over 14 (as well as his/her parents/tutors) is entitled to obtain from the data controller or the website owner the deletion or blocking of unlawful contents. The law provides for a specific role of the *Garante* as is the case with the request being not satisfied by 24 hours, the same request can be submitted to the *Garante* who will remove the content within 48 hours.

33. It is particularly important that national laws only allow surveillance following judicial orders granted on the basis of reasonable suspicion of the target being involved in criminal activity, that unlawful data processing in the digital scenario is penalised in the same way as the violation of the traditional confidentiality of correspondence and that all institutions and businesses holding personal data apply the most effective security measures available.

34. Data protection authorities play a crucial role in respect of oversight mechanism and the enforcement of data subject rights. Cooperation among competent autorities of different states should be considered of a particular importance to ensure coordinated mechanisms capable to react to the challenges of extra-territorial processing.

(2783 words)

Annex No. 1

Relevant national Authorities

35. Against this background, it is important to provide an overview of the role and work carried out particularly by AGCOM, standing for the Communication Regulatory Authority[1] and the Italian DPA, standing for the Italian Data Protection Authority.

The Communication Regulatory Authority (acronym in Italian, AGCOM)

36. The Communication Regulatory Authority is an independent Authority, established by Act 249/1997.

37. Independence and autonomy are key elements that characterize its activities and resolutions. AGCOM is first and foremost a guarantee Authority: its law of establishment entrusts the Authority with the double task of ensuring the correct competition of operators on the market and of protecting consumers' fundamental freedoms.

38. The Communication Authority is a "convergent" Authority. As such, it performs regulatory and supervisory functions in the telecommunications, audiovisual, publishing and, more recently, postal sectors. The profound changes brought about by the digitalization process, which has ensured the uniform broadcast of audio (including voice), video (including television) and data (including Internet access), are the basis for the choice of convergent model, as adopted by the Italian legislator and shared by other sector Authorities, such as Ofcom in Great Britain and Fcc in the United States.

39. Like the other Authorities provided for by the Italian legislation, the AGCOM report on its work to the Parliament. The latter established this Authority's powers, defined the statute and elected the members (Authority's bodies are: the President, the Commission for infrastructures and networks, the Commission for services and products, the Council. The Commissions and the Council are collegial bodies. The Commissions are made up of the President and the two Commissioners. The Council is composed of the President and all the Commissioners).

40. On a more specific note, Act 215/2004[2], which deals with the mass media and information sector and covers possible conflicts of interest, including between government responsibilities and professional and business activities in general, details *inter alia* the powers, functions and procedures of the independent administrative Authorities responsible for oversight, prevention and imposing penalties to combat such cases, together with the applicable penalties:

- For companies in general, this responsibility lies with the Anti-trust Authority established by Act 287/1990 (Art. 6);
- For companies of the printed press and media sector, the responsibility lies not only with the above Authority but also with AGCOM, as instituted by Act 249/1997.

    - The above Authorities are characterized by their neutrality with regard to the parties with conflicting interests to be resolved and third parties, and are therefore *iusdicenti* in any relevant conflicts. Specifically, Act 215/2004 entrusts AGCOM to conduct audits against companies operating in the Integrated

[1] https://www.agcom.it/

[2] Because of its particular nature, the mass media and information sector is the subject matter of a number of specific provisions in the law under reference (Article 7). These particular provisions do not replace the general rules governing any type of company, but are additional to them.

Communications System (acronym, SIC) and are headed by the holder of governmental position (or by relatives).

- The SIC comprises all the main media business sectors, and may be considered to be the result of the multimedia convergence process in which apparently heterogeneous media (radio, television, newspapers, the Internet, cinema) are gradually drawing closer together and becoming integrated[3].

41. As for RAI, the public broadcasting service, a parliamentary commission ensures, inter alia, respect for pluralism. It is, however, AGCOM to oversee and ensure RAI's compliance with primary and secondary level provisions, with regard to pluralism and public service-related obligations.

42. AGCOM has been also entrusted with all those functions of a regulatory and control nature, relevant to the postal sector, in accordance with Art.1, paras.13 and 14, of Law Decree No. 201/2011, as converted into law (with amendments) by Act No. 214/2011.

43. With regard to intellectual property, AGCOM has introduced rules on the protection of copyright by Resolution (No.680/13/CONS), dated December 12, 2013, by which it identifies its jurisdiction in respect of those breaches occurring on electronic communications networks in accordance with Legislation on Copyright (Act No. 633/41 - in particular Article 182 bis, by which both this Authority and SIAE are entrusted, within their respective responsibilities, with supervisory powers) and Legislative Decree on Electronic Trade (Act No.70/2003 - entrusting AGCOM with the power to order the intermediary service providers to put an end to the violations committed in the network).

- With specific regard to the audiovisual media services, it should be stressed that Parliament has entrusted the above Authority with specific regulatory and normative powers in accordance with Art.32bis of Legislative Decree No. 177/2005 (entitled "Consolidated Text on Audiovisual and Radio Media Services").

<u>The Italian DPA</u>

44. The *Garante*, i.e. the Italian Data Protection Authority (DPA), is an administrative independent authority set up by the "Privacy Act" (675/1996, now merged into the consolidated Personal Data Protection Code).

- Similar authorities have been set up in all EU countries pursuant to Article 8 of the Charter of Fundamental Rights of the European Union.

45. The *Garante* is tasked with ensuring the protection of fundamental rights and freedoms as regards the processing of personal data along with respect for individuals' dignity. The *Garante* handles citizens' claims and reports and supervises over compliance with the provisions protecting private life. It decides on complaints lodged by citizens and is empowered to prohibit, also of its own motion, any processing operation that is unlawful or unfair. It can perform inspections, impose

[3] Act 112/2004 has effectively moved forward the switch from analogical to digital broadcasting, with the aim of increasing the number of TV channels (a process initiated in 2008). This has actually given greater independence and organizational autonomy to the public radio and television broadcasting service franchisee. It has placed RAI on an equal footing with all other joint stock companies, also in terms of their organization and management (Article 20 (1)). In this context, mention should be made also of the following: The start-up of terrestrial digital broadcasting as a result of Act 112/2004 has increased the number of channels free of charge by between four-fold and six-fold (as of 2014), and has consequently increased the television offering and enhanced pluralism — bringing Italy to be one of the countries with the highest number of channels ever, in the world.

administrative penalties, and issue opinions in the cases mentioned by the Data Protection Code. It can also draw Parliament and Government's attention to the desirability of regulatory measures concerning personal data protection (additional information in English is available on *Garante*'s website: http://www.garanteprivacy.it/web/guest/home_en).

Annex No. 2

General background

46. The (rigid) Basic Law of Italy (1948) determines the political framework for action and organization of the State. The fundamental elements or structural principles of the constitutional law governing the organization of the State are as follows: Democracy, as laid down in Article1; the so-called *personalistic* principle, as laid down in Article 2, which guarantees the full and effective respect for human rights; the pluralist principle, within the framework of the value of democracy (Arts. 2 and 5); the importance of work, as a central value of the Italian community (Arts. 1 and 4); the principle of solidarity (Article 2); the principle of equality, as laid down in Article 3 (it is also the fundamental criterion applied in the judiciary system when bringing in a verdict); the principles of unity and territorial integrity (Article 5); and above all the relevant principles, including the social state/welfare, the rule of law and the respect for human rights and fundamental freedoms, such as freedom of correspondence, freedom of movement, freedom of religion or belief, and freedom of opinion and expression.

47. The Italian legal system aims at ensuring an effective framework of guarantees, to fully and extensively protect the fundamental rights of the individual. Indeed, we rely on a solid framework of rules, primarily of a constitutional nature, by which the respect for human rights is one of the main pillars.

48. Within our national system of human rights protection, mention has to be made, among others, of the Italian constitutional court that deals only with infringements of a constitutional level (The constitutional court consists of fifteen judges; one-third being appointed by the President of the Republic/Head of State, one-third by the Parliament in joint session, and one-third by ordinary and administrative supreme court)[4]. The constitutional court exercises its duty as one of the highest guardian of the Constitution in various ways. It becomes active when it is called on. For example, it supervises the preliminary stages of referenda and is competent in case of presidential impeachment. Complaints of unconstitutionality may be submitted to the Italian Constitutional Court by central and local authorities claiming that a state or a regional Act might be unconstitutional. Therefore, the Court monitors Authorities to see whether they have observed the Constitution in their actions. It also arbitrates in cases of disagreements between the highest State's organs and decides in proceedings between central and local Authorities.

- Procedurally, the court must examine *ex officio* (the prosecutor) or upon request of the plaintiff/defendant whether the provisions to be applied are in compliance with the Basic Law. When the court considers that an act is unconstitutional, such evaluation brings to a suspension of the *a quo* proceeding. Accordingly, a decision is made by the Court itself, pursuant to Art. 134 of the Italian Constitution. The constitutional court decides (and its decisions cannot be appealed) disputes: 1. concerning the constitutionality of laws and acts with the force of law adopted by state or regions; 2. arising over the allocation of powers between branches of government, within the state, between the state and the regions, and between regions; 3. on accusations raised against the head of State in accordance with the Constitution. More generally, this Court decides on the validity of legislation, its interpretation and if its implementation, in form and substance, is in line with the Basic Law. Thus, when the court declares a law or an act with the force of law unconstitutional, the norm ceases its force by the day after the publication of its decision.

[4] The constitutional court consists of fifteen judges; one-third being appointed by the Head of State, one-third by the Parliament in joint session, and one-third by ordinary and administrative supreme court.

CONCLUSIONS

Italian Authorities take this opportunity to reiterate their firm willingness to continue cooperating fully with all UN Special Procedures.