National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

ITALY

Version of 13 October 2014

Cooperazione per lo Sviluppo dei Paesi Emergenti (COSPE)
Marialuisa Gambini

Summary

[1]. With Law no. 124 of 3 August 2007[1], on "*Information System for the security of the Republic and new rules on State secrets*", the Parliament launched a comprehensive reform of the national intelligence authorities by creating the "Information System for the security of the Republic" in order to preserve the Republic from all kinds of danger and threat coming both from within and outside the country.

[2]. Pursuant to Article 2, of the above law, the "Information System for the security of the Republic" is a complex set of bodies and authorities – that operate at the national level (there are no decentralised or regional authorities) without geographical limitations – consisting of: the President of the Council of Ministers (has overall responsibility for the entire national security policy); the Inter-ministerial Committee for Security of the Republic (CISR); a delegated Authority (normally, if established, it is coordinated by an Under-Secretary to whom the Presidency of the Council of Ministers may delegate functions concerning intelligence); the Department for Security Information (DIS);the Information and External Security Agency (AISE) and the Information and Internal Security Agency (AISI) (these last two agencies are expressly referred to as "Information Services for Security").

[3]. When referring to the Parliamentary Committee for the Security of the Republic (COPASIR), the dispositions concerning are included in articles 30, 31, 32, 33 and 34 of Law 124/2007. Furthermore, Article 30, of Law no. 124/2007 gives COPASIR the function to verify – "*systematically and continuously*"– that the activity of the Information System for the security of the Republic is carried out in accordance with "*the Constitution, the laws, solely in the interest and for the defence of the Republic and its institutions*". The Committee is composed of five members of the Chamber of Deputies and five senators appointed within twenty days of the start of each term in office by the Presidents of both Houses of Parliament, in proportion to the number of members of each parliamentary group, guaranteeing the equal representation of the majority and the opposition, and taking into account the specific tasks of the Committee. The Committee has the task to ensure, among other things, that the functions delegated to Agencies are not performed by other bodies. COPASIR also has wide advisory powers on secondary legislation concerning the intelligence sector and extensive supervisory powers: it is able to obtain information not only from the judiciary, as an exception to keeping details of investigations secret until they are concluded, and from public and private entities, as an exception to the obligation of professional secrecy, but also from individuals belonging to the Services, as an exception to the protection of State secret. It can also arrange inspections of the offices of the Information System, though after giving prior notification to the President of the Council of Ministers. Article 33, of Law no. 124/2007 also provides for broad reporting obligations on the Information Services (some of which periodically) towards the COPASIR. The following must be communicated, *inter alia*, to the Committee: the semi-annual report on the activities of the Information Services for Security, including an analysis of the situation and of the security hazards; the cases where "*functional guarantees*" can be claimed (i.e. the causes of justification of behaviour that might otherwise constitute a crime);the cases where classification as State secret can be claimed; requests for telephone-tapping made by the Services and the decisions of the President of the Council of Ministers on the requests by the judiciary to use telephone-tapping conducted on devices belonging to the Services (the President of the Council of Ministers can prevent such use by the judiciary by classifying the material in question as State secrecy); the various archives held by the Services (rightful, only insofar as they are communicated to COPASIR). Lastly, the Committee has the power to determine the illegal behaviour by the Services, because it can order the

[1] Italy, Law no. 124 of 3 August 2007 on "*Information System for the security of the Republic and new rules on State secrets*" (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto). Available at: *www.camera.it/parlam/leggi/07124l.htm*(17-07-2014).

President of the Council of Ministers to conduct internal investigations in the presence of a *fumus* of illegality, the results of such investigations are submitted, in their entirety, to the Committee.

[4]. Law no. 124/2007 does not provide specific judicial or non-judicial remedies for an individual subjected to surveillance: in fact, as discussed below, control by the judiciary is provided only as a precautionary measure in cases of acquisition of telephone or ICT traffic data or same telephone, ICT or environmental communications by the Services on individuals.

[5]. At the moment, official information seems to exclude, on the one hand, a direct involvement of Italy in the scandal known as "*Datagate*", given that it did not take part even in the European system of mass surveillance of communications and, on the other, the existence of large scale data acquisition programmes carried out by the national intelligence services. Moreover, even in the working Document of the Commission on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE) on the "*Relationship between surveillance practices in the EU and in the United States and the EU provisions on data protection*,[2]it is stated that *"the United States, United Kingdom, Sweden, France and Germany have the means to connect to the Internet backbone cables and collect all the traffic for a certain period of time('full take', NSA and GCHQ) or part of it (FRA, DGSE, BND) and at least the Netherlands seems to be working on a similar programme*", and this without, however, mentioning Italy.

[6]. On the other hand, massive tapping of huge traffic flows would not be possible in Italy (hence it would be difficult for an Italian Intelligence Service to freely operate in a context of transnational tapping) as there are strict legal restrictions which constitute a guarantee of protection for citizens. In any case, national legislation imposes – even for tapping performed by the Services –, not only a preventive jurisdictional control and an obligation of the Services to take responsibility for the legality of their own actions before the parliamentary supervisory body, but also very specific enabling conditions, such as the specific need to prevent serious crimes or documented need to protect national security in relation to concrete and well-grounded dangers[3].

[7]. Furthermore, according to Article 4 of Legislative Decree no. 144/2005[4], the National Information Services for Security (specifically identified as AISE -Agency for Information and External Security and/or AISI - Agency for Information and Internal Security) may carry out tapping activities and preventive controls on communications (i.e., phone calls, paper and electronic mail, phone records *etc.*) "*when these are deemed essential for performing the tasks assigned to them*", pursuant to Article 226 of the Implementing provisions of the Code of Criminal Procedure[5].In other words, only if they

---

[2] Available at: *www.istrid.it/articoli/relazione-tra-le-prassi-di-sorveglianza-nellue-e-negli-stati-uniti-e-le-disposizioni-dellue* (17-07-2014).

[3]On the contrary, as clarified in a speech by the Data Protection Authority (DPA): "many US laws permit the acquisition for intelligence purposes, even on a large scale and preventively (i.e. in the absence of evidence of a crime and even of danger), of personal data (both in terms of the external character and content) related to direct communications with the United States or processed by providers that are subject to US jurisdiction, in some cases without even judicial validation (Executive Order 12333) or, at the most, on the basis of a purely simple authorisation (FISA, Patriot Acts) by a special judge, following a secret procedure, without any cross-examination and generally "submissive" to the demands of the executive branch. Authorisations would be issued *de plano* in 75% of cases, according to the US declaration". Available at:*www.key4biz.it/files/000248/00024810.pdf*

[4] Italy, *Urgent measures to fight international terrorism,* Legislative Decree no. 144 of 27 July 2005, Article 4, converted into Law no. 155 of 31 July 2005, as it stands in the current text amended by Law no. 133 of 7 August 2012, available at: *www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133* (23-07-2014).

[5]Available at:

serve to ensure the defence of the independence, integrity and security of the Republic from threats coming from abroad or the defence of the internal security of the Republic and its democratic institutions from all kinds of threats, subversive activity and forms of criminal or terrorist aggressions. Moreover, this is possible only when referring to single/specific individuals and on the condition that a prior judicial authorisationis issued (by the office of the Prosecutor General at the Court of Appeal of Rome) and, in any case, for a limited period of time (40 days renewable for later periods of 20 days if the above legal requisites remain valid).The request for authorization specifies the individual to be placed under surveillance.

[8]. Besides, the general rules of the *Code on the protection of personal data*[6] are applied to the processing of data collected by the Information and Security Services (AISE and/or AISI) for the purposes of State security, including the principles of necessity, purpose, legality, relevance and updating; the prohibition of profiling; a particular system of compensation for damages caused by unlawful data processing and the duty to ensure safety (Articles 1 to 6; and Articles 11, 14, 15, 31, 33, 58, 154, 160 and 169).Particularly relevant is the attribution to the Data Protection Authority (DPA), pursuant to Article 160 of the aforementioned Code, of extensive powers of inspection, in line with the provision that makes it impossible for the Services to refuse access to information by a delegated representative of the DPA in charge of the inspections, on the grounds that the requested information is 'classified' or 'secret'. In cases where the documents consulted are classified or if reporting the outcome of the inspection may affect the security of the State, no feedback will be given to the person who had made the complaint to the DPA that led to the inspection. Nevertheless, the DPA may request the adoption of appropriate measures or assess the consequences of any ascertained unlawful behaviour (Article 160, paragraph 2, of the aforementioned Code).

[9]. The current regulatory framework explains why in Italy, public debate on the issue of large-scale surveillance of communications carried out by National Intelligence Authorities was almost entirely absent – as can be indirectly inferred also from the Report of 21 February 2014 presented by the LIBE Committee: "*Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*"[7] – and consequently, few public and institutional initiatives have been undertaken on the subject.

[10]. At the Parliamentary level, the **Parliamentary Committee on the Security of the Republic** (COPASIR) carried out a series of hearings to find out whether there had been an "Italian *Datagate*". In particular, worth noting was the hearing of the DPA by the Committee on 23 July 2013, – pursuant to Article 31, paragraph 3, of Law no. 124 of 2007[8] –, in relation to the implications for the rights of EU citizens, of the collection of personal data for purposes of intelligence, carried out according to the *Foreign Intelligence Surveillance Act* (FISA) and the relationship between data protection and data processing for the purposes of State security in the Italian legal order, with particular regard to the so-called

www.diritto24.ilsole24ore.com/guidaAlDiritto/codici/codiceProceduraPenale/articolo/1229/art-226-intercettazione-e-controlli-preventivi-sulle-comunicazioni.html(21-07-2014).

[6] Italy, Code on the protection of personal data (*Codice in materia di protezione dei dati personali*), Legislative Decree no. 196 of 30 June 2003), available at: *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248* (05-08-2014).

[7] EP, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in the fields of Justice and Home Affairs. Available at: *www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN* (18-08-2014).

[8]Available at: *www.camera.it/parlam/leggi/07124l.htm*(17-07-2014).

power of "systematic access" by the Services to private and public databases[9], which will be discussed further below.

[11]. A more recent development that is worthy of note was the announcement in the **Chamber of Deputies**[10]- during the session of 30 April 2014 –, of the transmission by the President of the European Parliament, of the text on the "*European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*". This text was assigned, pursuant to Article 125, paragraph 1, of the Regulation of the Chamber of Deputies[11], to the First Joint Commission(*Constitutional Affairs*) and the Third Joint Commission (*Foreign Affairs*), as well as transmitted to the Fourteenth Commission (*European Union Policies*) for an opinion. However, since the report was assigned as described above, no specific activity or initiatives have been taken to date by the aforementioned Commissions.

[12]. In any case, the issue of the possible existence in Italy of a system that is similar to *Datagate* or which may degenerate (this is an assumption of the author and of part of public opinion not supported by any concrete evidence and as such, a mere potential risk!) into a collection of data on a large scale (i.e. based on generalisedand indiscriminate forms of data acquisition, not related to any evidence of crime and aimed at achieving a constant surveillance of citizens' lives) was raised by **Article 13, paragraph 2, of the law on the reform of the Intelligence services**[12], which provides that: "*A specific regulation adopted after consultation with various administrations and interested parties, will define provisions that are necessary to ensure access by the DIS, the AISE and the AISI to computer-based archives of public administrations and authorities providing, under authorisation, concession or contract, services of public utility and it will also specify, in any case, the technical procedures that are necessary to check access to personal data, even afterwards*".

[13]. In order to implement the above provision, a **Decree of the President of the Council of Ministers was issued on 12 June 2009** containing "*Rules governing the procedures and criteria for access by the DIS, the AISE and the AISI to computer-based archives of public administrations and authorities providing, under authorisation, concession or contract, services of public utility*"[13]. However, the text of the Regulation is not publicly available, because only a statement about it was published in Official Gazette no. 154 of 6 July the 2009[14]– as often happens in cases of official documents relating to national security.

[9]Available on the website: http://www.senato.it/leg/17/BGT/Schede/ProcANL/ProcANLscheda27525.htm (17-07-2014).
[10]Available at: *www.camera.it/leg17/410?idSeduta=0221&tipo=documenti_seduta*(17-07-2014).
[11]Available at: *http://leg16.camera.it/437?conoscerelacamera=237*(21-07-2014).
[12] Italy, Law no. 124 of 3 August 2007 on "Information System for the security of the Republic and new rules on State secrets" (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*). Available at: *www.camera.it/parlam/leggi/07124l.htm*(17-07-2014).
[13] Italy, Decree of the President of the Council of Ministers of 12 June 2009 containing "Rules governing the procedures and criteria for access by the DIS, the AISE and the AISI to computer-based archives of public administrations and authorities providing, under authorisation, concession or contract, services of public utility. Available at: *www.parlamento.it/963?documento=37*(4-08-2014).
[14] The aforementioned decree of the Prime Minister was specifically requested by the author from the DPA(see Doc. 2 attached) and the Head of institutional communications of the Information System for the Security of the Republic (see Doc. 3). In particular, the latter replied explicitly that the requested document cannot be disclosed to the public (see Doc. 5 attached).

[14]. Above all, the so-called "Monti Decree"[15] introduced a special provision which allows access by Intelligence Agencies to databases managed by "*private operators providing public communications networks or electronic communications services accessible to the public*" as well as "*those who manage critical infrastructures of national and European relevance, the functioning and efficiency of which depend on computer and telecommunications systems*" (Article 11, paragraph 1, letter c).According to the wording of the provision, it would allow the Intelligence Agencies almost indiscriminate access and without prior authorisationby the Courts (as required indeed in the cases mentioned above and, in general, for phone-tapping) to all the databases managed by the operators of such services. This power which is to be exercised only with regard to "*those databases that are of interest for cyber security that falls under each Agency's responsibility, in the cases provided for by the law no. 124/2007*",is regulated only on the basis of "*special Agreements*" previously signed by the Services and the above mentioned private operators[16].It seems that only at a later stage will notice of such Agreements be given to COPASIR so that it can exercise its supervisory powers.

[15]. For that reason also, and in order to mitigate the risk that the "Monti Decree" may exploit a *loophole* in the law without any accompanying rules meant to safeguard what happens to these data, on 11 November 2013, the DPA –through an initiative that has no precedent in other EU countries –signed a **Memorandum of Understanding**[17] with the Department for Security Information (DIS) of the Presidency of the Council of Ministers aimed at further strengthening the protection of citizens in the field of intelligence as well, by regulating certain informative procedures that are functional to the exercise of their respective powers. As the DPA President, Antonello Soro, clarified, the Memorandum represents "*'a positive response' to the concerns raised by* Datagate*, an answer capable of consolidating the supervisory activities of the DPA and allow a supervision of the archives used by the Services*"[18]. From this point of view, the Memorandum strengthens the prerogatives of the DPA, making them more in line with the peculiarities that currently characterisethe activities of Information Agencies and their so-called powers of "systematic access"[19], as extended by Law no. 133 of 2012 and in accordance with the global trend linked to the growing dangers of cyber threats. This way, the measure takes another step forward in the direction of transparency of the "intelligence sector" already initiated by the reform of the Intelligence Services (Law no. 124 of 2007) and in support of a shared culture on security.

[16]. More specifically, given that the so-called "*Datagate*" has caused renewed attention by different supervisory bodies to the processing of personal data by the Intelligence Services, the definition of the Memorandum aims to respond to the need to render the supervision by the DPA, which is already

---

[15] Italy, Decree of the President of the Council of Ministers of 24 January 2013: "Directive containing guidelines for cyber-security and national IT security". (*D.P.C.M. 24 gennaio 2013: «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*). Available at: *www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg*(21-07-2014).

[16]The contents of these "*Agreements*" – specifically requested also from the DPA (see Doc. 2 attached) and the Head of institutional communication of the Information System for the Security of the Republic (see Doc. 3 attached)– are protected as *classified* documents. In particular, the latter replied explicitly that the requested document cannot be disclosed to the public (see Doc. 5 attached). According to media sources however, within a few months beginning from January 2013, the Agreements stipulated between the Services and private telecommunications giants (such as Telecom) were about ten, with a one-year duration and based on a model made up of 12 Articles, protected as *classified* information (*www.repubblica.it/tecnologia/2013/06/17/news/datagate_italiano-61291652/*).

[17] The Document – which was specifically requested from the same two institutions as in the previous footnote, are cannot be disclosed to the public because it is classified. All that we have been able to access on suggestion of the DPA is the press release by the Presidency of the Council of Ministers that reported the signing of the Memorandum of Understanding (*www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=73621*(01-08-2014) and the statement by the DPA after signing the Memorandum *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2746204*(01-08-2014).

[18]Available at: *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2792187* (23-07-2014).

[19]As stated in the annual speech by the DPA President, Antonello Soro to Parliament; available at: *http://194.242.234.211/documents/10160/0/Relazione+annuale+2013+-+Discorso+del+Presidente.pdf*(17-07-2014).

provided under the existing law, more systematic and together with COPASIR and the judicial Authority (the latter with regard to communications data), complete the range of protection measures meant to safeguard the processing of personal data for purposes of intelligence. For this purpose, the Memorandum of Understanding reviews all existing provisions on inspections of the Intelligence services by the DPA, with particular regard to access to databases of administrations and operators of public utility services and access to databases for purposes specified in the directive on cyber security.

[17]. Secondly, the Memorandum highlights the procedures for implementing the inspections by the DPA of the Information Agencies (AISE and/or AISI) and provides that a programme of consultation of the electronic archives to which DIS and the Information Agencies have access to, pursuant to Article 13, paragraph 2, of Law no. 124 of 2007, is communicated to the DPA. Acquisition of data pursuant to Article 11 of the "Monti Decree", should also be communicated to the DPA in the case that such access has led to the identification of the subject by the Information Agencies. In order to protect the classified character of the information from the "intelligence sector", the agreement also provides that documents sent to the DPA are stored using procedures that are capable of ensuring their classified nature.

[18]. Thirdly, the Memorandum accords the "*intelligence sector*" the possibility of using –besides the cases already provided for by the law –, the advisory activities of the DPA on issues related to the processing of personal data. Lastly, it provides for the appointment of one or more representatives of each party for the implementation of the Memorandum and it sets a two-year duration and the possibility of updating the same in the case of new laws and regulations on the specific subject.

[19]. Furthermore, as reported in the Annual Report for the year 2013 presented on 10 June 2014[20],following the news about the so-called "*Datagate*",–the DPA carried out a series of information activities and discussions with the Government, in order to minimize the risks for Italian citizens of acquisition of their data for intelligence purposes.

[20]. In particular, on 22 October 2013, in the aftermath of the approval by the LIBE Committee of the European Parliament, of the proposal for a regulation on the protection of personal data[21], the DPA, in a **letter to the President of the Council of Ministers[22]**, pointed out the need to ascertain whether electronic espionage conducted by NSA involved, albeit incidentally, Italian citizens. In the same letter, the DPA highlighted also the need to adopt effective means of protection of personal data processed for security purposes, aware of and in agreement with the European objective of strengthening the tools for police and judicial cooperation. The letter expressly points out that "*the legislation implementing the principles of the Code on the protection of personal data, as regards data processing for purposes of justice, police or national security, has not yet been adopted*", and it also underlines that "*the persistence of the above mentioned regulatory gaps in such delicate areas, ten years after entry into force of the Code, is likely to undermine the objectives pursued and weaken the right to protection of personal data of citizens processed by State authorities in their exercise of far-reaching public authority powers, thereby undermining citizens' confidence in State institutions*".

[20]Available at: *http://194.242.234.211/documents/10160/0/Relazione+annuale+2013.pdf*(17-07-2014).
[21]Available at: *www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//IT*(23-07-2014).
[22]Available at: *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2708275* (17-07-2014).

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
[23]Law no. 124 of 3 August 2007, on «Information System for the security of the Republic and new rules on State secrets» (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*»). – *Act of the Parliament*	Not expressly specified, so anyone could be subjected to it. In fact, Article 13(2)grants National Intelligence Authorities access to databases and archives of public administrations and other subjects that provide public utility services.	This point is neither expressly specified nor can it be deduced from other laws.	AISE is entrusted with the task of searching and processing in the areas of competence of all relevant information to the defense of the independence, integrity and security of the Republic, also in implementation of international agreements, from threats from	Article 13, paragaph 2 does not specify whether *prior*/*ex-post* judicial warrant is needed in order to undertake surveillance. A specific regulation should determine the technical procedures that are necessary to check access to personal data, even afterwards.	This point is neither expressly specified nor can it be deduced from other laws.	No limitations are expressly providedfor by the law with regard to nationality, national borders, time limits, quantity of data flow *etc*. Potentially all information contained in the databases and archives could be accessed.	The law does not allow for mass surveillance in another country (EU MS or third countries). It refers exclusively to national public administrations and national subjects that provide, under the authorisation, concession or contract, public utility services.

[23]In Italy, a regulation that allows for mass surveillance does not exist (see Summary above for details). However, it is useful to refer to the act setting-up national intelligence services: available at: *www.camera.it/parlam/leggi/07124l.htm* (21-07-2014).

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			abroad (art. 6.1 of law 124/2007). AISI is entrusted with the task of searching and processing in the areas of competence of all relevant information to defend, even in the implementation of international agreements, the internal security of the Republic and democratic institutions by the Constitution from every threat, subversive activity and all forms of aggression, criminal or				

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			terrorist. (art 7.1 of law 124/2007).				
Article 11, paragraph 1, letter *c*, of Decree of the President of the Council of Ministers 24 of January 2013: "Directive containing guidelines for cyber-security and national IT security". (*D.P.C.M. 24 gennaio 2013: «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*). – *Act of the Government*	Not expressly specified by the Decree, so anyone could be subjected to such surveillance.	This point is neither expressly specified nor can it be deduced from other laws.	The Article 11, paragraph 1, letter *c*, of this Presidential decree only states that National Intelligence Authorities are allowed to access databases for their respective purposes of cyber security, in the cases provided for by Law no. 124/2007. This power may therefore be exercised whenever it is needed to protect the interests of the Republic. However, this does not allow for	Does not specify whether *prior* / *ex-post* judicial warrant is needed in order to undertake surveillance. According to art. 11, the access is allowed only under specific conditions (for cybersecurity and in the respect of DP principles), and is limitated to incident of electronic nature, such as the violation of security or integrity of electronic systems). Moreover, for preventive interceptions, an authorization by the Judicial Authority	Not expressly specified. In fact, access to databases is only regulated on the basis of mere «*Agreements*» signed by the IntelligenceServices with private operators. It must only give notice of the agreements to the Parliamentary Committee for the Security of the Republic (COPASIR) so that it can exercise its supervisory powers.	Does not expressly provide limitations regarding nationality, national borders, time or quantity of data flow *etc*.	Does not allow for mass surveillance in another country (EU MS or third countries). It refers exclusively to national public administrations and national subjects that provide, under the authorisation, concession or contract, public utility services.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			the NIS to obtain neither personal data nor metadata of personal communication contained in the databases.	must always be granted first (in the State, this is the sole competence of the General Attorney of the Court of Appeals in Rome).			
Legislative Decree no. 144 of 27 July 2005, Urgent measures to fight international terrorism, *(Decreto legge 27 luglio 2005, n.144, recante misure urgenti per il contrasto del terrorismo internazionale)* converted into Law no. 155 of 31 July 2005, as it stands in the current text amended by Law	Not expressly specified by the Decree.	This point is neither expressly specified nor can it be deduced from other laws.	Fight gainst international terrorism	Does not specify whether *prior* / *ex-post* judicial. According to art. 11 of the Decree of the President of the Council of Ministers 24 of January 2013(?), the access is allowed only under specific conditions (for cybersecurity and in the respect of DP principles), and is limitated to incident of electronic nature, such as the violation of security or	Not expressly specified.	Does not expressly provide limitations	Does not allow for surveillance in another country (EU MS or third countries).

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
no. 133 of 7 August 2012				integrity of electronic systems). Moreover, for preventive interceptions, an authorization by the Judicial Authority must always be granted first (in the State, this is the sole competence of the General Attorney of the Court of Appeals in Rome).			
Decree of the President of the Council of Ministers of 12 June 2009 containing "Rules governing the procedures and criteria for access by the DIS, the AISE and the AISI to computer-based archives of public	Text not available to the public.	Text not available to the public.	Text not available to the public.	Text not available to the public.	Text not available to the public.	Text not available to the public.	Text not available to the public.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
administrations and authorities providing, under authorisation, concession or contract, services of public utility (*Decreto del Presidente del Consiglio dei Ministri del 12 giugno 2009*).							
Code of Criminal Procedure		The intercepts are first of all contemplated as a means of gathering evidence in the pursuit of responsibilities relating to certain offenses (articles 266 and following). Preventive intercepts are listed under art.					

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
		226. Such intercepts should have as a goal to prevent determinated crimes.					

B- Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protectionapply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protectionapply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
In Italy, there are no specific law(s) providing for the protection of privacy and data protection against mass surveillance. To date, it should be noted the announcement in the **Chamber of Deputies**[24]– during the session of 30 April 2014 –, of the transmission by the President of the European Parliament, of the text on the "*European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*" which was assigned, pursuant to Article 125, paragraph 1, of the Regulation of the Chamber of Deputies, to the First and Third Joint Commissions (*Constitutional Affairs and Foreign Affairs*) and for an opinion, to the Fourteenth Commission (*European Union Policies*) .	/	/	/
Although, there are no specific law(s) in Italy providing for the protection of privacy and data protection against unlawful mass surveillance, it	According to Article 15 of Italian Constitution, "*Freedom and confidentiality of*	The rule on individual protection of privacy and data protection applies equally to	The rule on individual protection of privacy and data protection applies only within

[24]Available at: *www.camera.it/leg17/410?idSeduta=0221&tipo=documenti_seduta*(17-07-2014).

is generally possible to invoke the application of the constitutional protection estabilished by Article 15 of the Constitution.	*correspondence and of every other form of communication is inviolable.* *Limitations may only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law.*" (see for example the guarantees established byArticle 226 of the Implementing provisions of the Code of Criminal Procedure[25]).	nationals, EU citizens and third country nationals.	the country. See Article 5 of the Personal Data Protection Code.
Although, there are no specific law(s) providing for the protection of privacy and data protection against unlawful mass surveillance, it is useful to point out the individual protection referred to in the Article 4 of Legislative Decree 144/2005[26].	According to Article 4 of Legislative Decree no 144/2005, National Information Services for Security (specifically identified as AISE - Agency for Information and External Security and/or AISI - Agency for Information and Internal Security) may carry out tapping activities and preventive controls on communications (i.e., phone calls, paper and electronic mail, phone records *etc.*) "*when these are deemed essential for performing the tasks assigned to them*", pursuant to Article 226 of the	The rule on individual protection of privacy and data protection applies equally to nationals, EU citizens and third country nationals.	The rule on individual protection of privacy and data protection applies only within the country.

[25]Available at: *www.dirittо24.ilsole24ore.com/guidaAlDiritto/codici/codiceProceduraPenale/articolo/1229/art-226-intercettazione-e-controlli-preventivi-sulle-comunicazioni.html*(21-07-2014).

[26] Italy, *Urgent measures to fight international terrorism*, Legislative Decree no. 144 of 27 July 2005, Article 4, converted into Law no. 155 of 31 July 2005, as it stands in the current text amended by Law no. 133 of 7 August 2012, available at: *www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133* (23-07-2014).

	Implementing provisions of the Code of Criminal Procedure[27].		
Although, there are no specific law(s) providing for the protection of privacy and data protection against unlawful mass surveillance, it is useful to point out the individual protection referred to in the Article 4 of Legislative Decree 144/2005[28].	According to Article 4 of Legislative Decree no 144/2005, National Information Services for Security (specifically identified as AISE - Agency for Information and External Security and/or AISI - Agency for Information and Internal Security) may carry out tapping activities and preventive controls on communications (i.e., phone calls, paper and electronic mail, phone records *etc.*) "*when these are deemed essential for performing the tasks assigned to them*", pursuant to Article 226 of the Implementing provisions of the Code of Criminal Procedure[29].	The rule on individual protection of privacy and data protection applies equally to nationals, EU citizens andthird country nationals.	The rule on individual protection of privacy and data protection applies only within the country.
Although, there are no specific law(s) in Italy providing for the protection of privacy and data protection against unlawful mass surveillance, it is useful to point out that the general rules of the *Code on the protection of personal data*[30] are applied to the processing of data collected by the	The main principles of the *Code on the protection of personal data* are applied to the processing of data collected by the Information and Security Services (AISE and/or AISI) for	The rule on individual protection of privacy and data protection applies equally to nationals or also to EU citizens and/or third country nationals.	The rule on individual protection of privacy and data protection applies only inside Italy.

[27]Available at: *www.diritto24.ilsole24ore.com/guidaAlDiritto/codici/codiceProceduraPenale/articolo/1229/art-226-intercettazione-e-controlli-preventivi-sulle-comunicazioni.html*(21-07-2014).

[28] Italy, *Urgent measures to fight international terrorism*, Legislative Decree no. 144 of 27 July 2005, Article 4, converted into Law no. 155 of 31 July 2005, as it stands in the current text amended by Law no. 133 of 7 August 2012, available at: *www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012;133* (23-07-2014).

[29]Available at: *www.diritto24.ilsole24ore.com/guidaAlDiritto/codici/codiceProceduraPenale/articolo/1229/art-226-intercettazione-e-controlli-preventivi-sulle-comunicazioni.html*(21-07-2014).

[30] Italy, Code on the protection of personal data (Codice in materia di protezione dei dati personali), Legislative Decree no. 196 of 30 June 2003), available at: *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248* (05-08-2014).

Information and Security Services (AISE and/or AISI) for the purposes of State security. In particular, art. 58 of legislative decree 196/2003 regulates the data processing done by the Information and Security Services.	the purposes of State security, including the principles of necessity, purpose, legality, relevance and updating; the prohibition of profiling; a particular system of compensation for damages caused by unlawful data processing and the duty to ensure safety. Specifically, are implemented the general principles of the law on privacy (Articles 1-6 of the Code), the method of treatment (Articles 11 and 14), the compensation for damage caused as a result of the processing of Personal Data (Art. 15), an estimate of the obligation to adopt measures to protect against the risk of destruction or loss of personal data, access or treatment not allowed (articles 31 and 33), the tasks of the Authority for the protection of personal data (art. 154), the investigation of the treatment of personal data related to Information and Security Services and to data covered by state secrecy (art. 160), and the system of penalties (Article 169). Provisions concerning the notification of processing to the DPA (Articles 37, 38 and 163) also apply for		

	treatments carried out by public entities for purposes of defense or security of the State on the basis of specific provisions of the law.		
Law 124/2007, "Information System for the security of the Republic and the new discipline of secrecy" ("*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto")*	This law contains special provisions in case of treatment of personal information by the Information and Security Services (Articles 26 and 33, paragraph 9), in fact implementing the general principle of necessity and purpose limitation that regulates the processing of personal data, stated in the Code of privacy, article 26 of Law no. 124/2007 has expressly provided that the collection and processing of news and information from the DIS and the agencies should be targeted exclusively to the pursuit of institutional goals of the information system security. For the pursuit of their institutional purposes, law n. 124/2007, provided in Article 13, inter alia, the possibility for the Information and Security Services to access electronic archives of public administrations and of providers of public services, in ways that also allow for the verification of access to the personal data, to be		

	identified by appropriate regulations.		

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Parliamentary Committee for the Security of the Republic (COPASIR)	Parliamentary oversight body.	Article 2, of Law no. 124 of 2007[31].	The Article 2, of Law no. 124 of 2007 gives the Parliamentary Committee for the Security of the Republic (COPASIR) the function of ensuring – "*systematically and continuously*" – that the activity of the Information System for the security is carried out in accordance with "*the Constitution, the laws, solely in the interest and for the defense of the Republic and its institutions*".	The Committee is composed of five members of the Chamber of Deputies and five senators appointed within twenty days of the start of each term in office by the Presidents of both Houses of Parliament, in proportion to the number of members of each parliamentary group and taking into account the specific tasks of the Committee[32].	The Committee has the power to ensure, among other things, that the functions delegated to Agencies are not performed by other bodies. COPASIR has also wide advisory powers on secondary legislation concerning the intelligence sector and penetrating control powers[33].

[31] Available at: www.camera.it/parlam/leggi/07124l.htm (21-07-2014).

[32] For details, see pages 88 and 93 of the "EP report of 2011 concerning the Parliamentary oversight of Security and Intelligence agencies in the European Union", available at:http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf(30-09-2014).

[33] For details, see pages 242 ss. of the "EP report of 2011 concerning the Parliamentary oversight of Security and Intelligence agencies in the European Union", available at:http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf(30-09-2014).

Department for Security Information (DIS).	Executive oversight mechanism.	Article 4, of Law no. 124 of 2007[34].	The DIS is a Department of the Presidency of the Council of Ministers, which has the task of supervising the activities of AISE and AISI on the correct application of provisions issued by the President of the Council of Ministers, as well the administrative protection of state secrets.It also has the task of promoting and diffusing a culture of security and institutional communication and providing guidelines on the unified management of the staff of the various structures. The DIS depends directly on the President of the Council of Ministers, except for those specific aspects delegated to the Under-Secretary at the Presidency of the Council of Ministers, responsible for intelligence.	The DIS consists of: 1) the General manager nominated solely by the President of the Council of Ministers, after consulting the Inter-ministerial Committee for Security of the Republic (CISR); 2) other Offices, such as-the Central Office for Security (UCSI), which deals specifically with administrative protection of State secrets, including the issuance or revocation of security clearance; -the Central Office of the archives, which coordinates, regulates and monitors the management of data held by the intelligence Services; - Inspection Office, which is responsible for exercising control on AISE and AISI, to ensure compliance with the laws and regulations on information activities for security and the directives and orders of	The President of the Council of Ministers and the Under-Secretary at the Presidency of the Council of Ministers responsible for intelligence both use the DIS for the exercise of their duties, in order to ensure full uniformity in the planning of information researchby the Information System for Security and analysis and operational activities of the Intelligence services. It coordinates also the activities of Information System for Security and monitors the results of the activities carried out by AISE and dall'AISI. It is regularly informed of the operations conducted by the Information Services for Security and it transmits to the President of the Council of Ministers, the reports and analysis produced by the former. It collects information, analysis and reports from the armed forces,the police,

				the President of the Council of Ministers; - the Training School, which is responsible for training operators of the agencies.	government departments and research institutions, including private private ones also.While it does not interfer in the exclusive responsibility of AISE and AISI to elaborate their operative research plans, it processes strategic analysis related to particular situations, and makes assessments and forecasts on the basis of sectoral contributions of AISE and AISI. The DIS also formulates, on the basis of the information and reports of other Services global analysis to be submitted to CISR, as well as information research projects, on which the President of the Council of Ministers decides, after acquiring the opinion of the CISR. It also promotes and guarantees through regular meetings, the exchange of information between the AISE/AISI

[34] Available at: *www.camera.it/parlam/leggi/07124l.htm* (21-07-2014).

					and the Police; communicates to the President of the Council of Ministers the information from such exchanges and the results of periodic meetings. It processes, in agreement with AISE and AISI, the plan of acquisition of human and materials resources and any other useful assets in the activity of the Information services for Security, to be approved by the President the Council of Ministers.

Memorandum of Understanding between the Department for Security Information (Dipartimento delle informazioni per la sicurezza - DIS) and the Data Protection Authority (DPA).	Conventional mechanism between a governmental and *an* independent authority.	None. The Memorandum was signed on a voluntary basis and it is simply based on the principle of loyal cooperation between Institutions of the Republic.	The Memorandum highlights the procedures for implementing the inspections of the Information Agencies (AISE and/or AISI) by the DPA and provides that: 1) a programme of consultation of the electronic archives to which DIS and the Information Agencies have access to, pursuant to Article 13, paragraph 2, of Law no. 124 of 2007, is communicated to the DPA; 2) the acquisition of data pursuant to Article 11 of the "Monti Decree", should also be communicated to the DPA in the case that such access has led to the identification of the subject by the Information Agencies.	Not expressly specified.	Not expressly specified. However, the Memorandum accords the "intelligence sector" the possibility of using – besides the cases already provided for by the law – , the advisory activities of the DPA on issues related to the processing of personal data.

Annex 3 – Remedies[35]

Article 13, paragraph 2, of Law no. 124 of 3 August 2007, on «Information System for the security of the Republic and new rules on State secrets»				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No	Not expressly specified	Not specified	/
Analysis*	No	Not expressly specified	Not specified	/
Storing*	No	Not expressly specified	Not specified	/
Destruction*	No	Not expressly specified	Not specified	/
After the whole surveillance process has ended	No	Not expressly specified	Not specified	/

[35] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: *http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection*.

Article 11, paragraph 1, letter *c*, of the Decree of the President of the Council of Ministers of 24 January 2013.				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No	Not expressly specified	Not specified	/
Analysis*	No	Not expressly specified	Not specified	/
Storing*	No	Not expressly specified	Not specified	/
Destruction *	No	Not expressly specified	Not specified	/
After the whole surveillance process has ended	No	Not expressly specified	Not specified	/

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: *http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection*.

In Italy the individual has no specific remedy at his/her disposalagainst unlawful mass surveillance. However, the individual subjected to surveillance may certainly obtain protection according to the general remedy estabilished by Article 2043 of the Civil Code[36] ("*Any malicious or negligent act that causes an unjust damage to others, obliges the subject who committed the act to pay damages*"), which allows to request for compensation also for an unlawful act (in this specific case, unlawful surveillance) made by a public authority. Also Article 152 of the of the *Code on the protection of personal data*[37] confirms that any disputes concernig an infringment of data protection provisions are attribuited to judicial Authorities.

Moreover, pursuant to Article 142 of the aforementioned Code, the individual may certainly obtain protection by applying to the DPA through a detailed complaint (letter *a*), a report (letter *b*) or a petiton (letter *c*)[38].

As described in the Summary and in Annex 2, the Memorandum of Understanding signed between the Department for Security Information (DIS) and the Data Protection Authority (DPA)[39] highlights the procedures for implementing the inspections of the Information Agencies (AISE and/or AISI) by the DPA and provides that:
1) a programme of consulting the electronic archives to which DIS and the Information Agencies have access, pursuant to Article 13, paragraph 2, of Law no. 124 of 2007, is communicated to the DPA;
2) the acquisition of data pursuant to Article 11 of "Monti Decree", should also be communicated to the DPA in the case that such access has led to the identification of the subject by the Information Agencies.

[36]Available at: http://www.altalex.com/index.php?idnot=36458 (30-09-2014).
[37] Italy, Code on the protection of personal data (*Codice in materia di protezione dei dati personali*), Legislative Decree no. 196 of 30 June 2003), available at: *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248* (05-08-2014).
[38]FRA (2014), "*Data Protection: redress mechanisms and their use - Italy*", available at: https://fra.europa.eu/sites/default/files/access_to_data_protection_remedies_country_it.pdf(04-10-2014).
[39] The Document – which was specifically requested from the same two institutions as in the previous footnote, are cannot be disclosed to the public because it is classified. All that we have been able to access on suggestion of the DPA is the press release by the Presidency of the Council of Ministers that reported the signing of the Memorandum of Understanding (*www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=73621*(01-08-2014) and the statement by the DPA after signing the Memorandum *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2746204*(01-08-2014).

Annex 4 – Surveillance-related case law at national level

Please provide a maximun of three of the most important national cases relating to surveillance.Use the table template below and put each case in a separate table.

Case title	None
Decision date	/
Reference details (type and title of court/body; in original language and English [official translation, if available])	/
Key facts of the case (max. 500 chars)	/
Main reasoning/argumentation (max. 500 chars)	/
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	/
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	/

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Parliamentary Committee for the Security of the Republic Comitato parlamentare per la sicurezza della Repubblica (COPASIR)	*Parliament*	The COPASIR does not have direct contact, but only the one of its members (see President Sen. Giacomo Stucchi: *giacomo.stucchi@senato.it*).	*http://www.parlamento.it/571?shadow_organo=406516*
President of the Council of Ministers Presidente del Consiglio dei Ministri	*Government*	Palazzo Chigi - Piazza Colonna, 370 - 00187 ROMA Phone: (+39) 06.67791 List of active email addresses at: *http://www.governo.it/AmministrazioneTrasparente/Organizzazione/TelefonoPostaElettronica/email.html*	*http://www.governo.it/Presidenza/*

Under-Secretary at the Presidency of the Council of Ministers with responsibility for intelligence Sottosegretario alla Presidenza del Consiglio dei Ministri con delega ai servizi segreti	*Government*	*domenico.minniti@senato.it*	*http://www.governo.it/Governo/Ministeri/ministri_gov.html*
Interministerial Committee for Security of the Republic Comitato interministeriale per la sicurezza della Repubblica (CISR)	*Government*	The head of institutional communication is Dr. Paolo Scotto di Castelbianco e-mail: *info@sicurezzanazionale.gov.it*	*https://www.sicurezzanazionale.gov.it/sisr.nsf/organizzazione/la-nostra-organizzazione-2/comitato-interministeriale-per-la-sicurezza-della-repubblica-cisr.html*
Department for Security Information Dipartimento delle informazioni per la sicurezza (DIS)	*Government*	The head of institutional communication is Dr. Paolo Scotto di Castelbianco e-mail: *info@sicurezzanazionale.gov.it*	*https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html*

Information and external security Agency Agenzia informazioni e sicurezza esterna (AISE)	*Government*	The head of institutional communication is Dr. Paolo Scotto di Castelbianco e-mail: *info@sicurezzanazionale.gov.it*	*https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html*
Information and internal security Agency Agenzia informazioni e sicurezza interna (AISI)	*Government*	The head of institutional communication is Dr. Paolo Scotto di Castelbianco e-mail: *info@sicurezzanazionale.gov.it*	https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aisi.html
Data Protection Authority (DPA) Garante per la protezione dei dati personali	*Indipendent agency*	Public Relations Office Phone: (+39) 06.69677.2917 certified e-mail: *urp@pec.gpdp.it* e-mail: *urp@gpdp.it*	*http://www.garanteprivacy.it/*

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources *(in accordance with FRA style guide)***:

1. Government/ministries/public authorities in charge of surveillance

Italy, Presidency of the Council of Ministers (Presidenza del Consiglio dei Ministri) (2013), *Trasparenza e sicurezza a garanzia del cittadino. Arriva il Protocollo d'intenti tra l'Autorità Garante per la Protezione dei dati personali e il Direttore Generale del DIS*, press release (*), 11 November 2013*, available at:http://www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=73621

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

Italy, Autorità Garante per la Protezione dei Dati Personali (2014), *Relazione per l'anno 2013 - La protezione dei dati nel cambiamento* (Annual Report 2013 - Data protection in transformation) , available at: http://194.242.234.211/documents/10160/0/Relazione+annuale+2013.pdf.

Italy, Autorità Garante per la Protezione dei Dati Personali (2013), Datagate: *lettera di Antonello Soro al Presidente del Consiglio dei Ministri Enrico Letta* (Datagate: Letter by Antonello Soro to the President of the Council of Ministers, Enrico Letta) (), Rome, 22 October 2013 available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2708275.

3. Non-governmental organisations (NGOs)

Italy, Altroconsumo (2013) *Anche l'Italia ha il suo "Datagate" – Reclamo presentato al Garante della privacy (*Even Italy has its Datagate – Petition filed with the DPA) (*)*, press release, 1 August 2013,available at: http://www.altroconsumo.it/hi-tech/nc/news/datagate-italiano.

4. Academic and research institutes, think tanks, investigative media report:

Bonini, C., Colaprico, P., Foschini, G. , Mensurati, M., Tonacci, F. (2013) *La via italiana al Datagate* (The Italian road to Datagate)(*), in: *La Repubblica*, 15 June 2013, available at: http://www.repubblica.it/tecnologia/2013/06/17/news/datagate_italiano-61291652/.

Chiusi, F. (2013) *Il Copasir snobba il Datagate* (COPASIR snobs Datagate) (*), in: *L'Espresso*, 2 July 2013, available at: http://espresso.repubblica.it/palazzo/2013/07/02/news/il-copasir-snobba-il-datagate-1.56124.

Bonini, C. (2013) *Datagate all'italiana: i 300 mila accessi dei Servizi Segreti ai nostri dati* (Datagate Italian style: the 300 thousand access by the Intelligence Services to our data),in: *La Repubblica*, 2 July 2013, available at: http://ricerca.repubblica.it/repubblica/archivio/repubblica/2013/07/02/servizi-nelle-banche-dati-italiane-in.html(26-07-2014)

Bianchini, E. (2013) *Il "Datagate" di Monti: blitz degli 007 sui dati possibile senza via libera dei giudici* (Monti's Datagate: blitz by Secret Service agents on data is possible without prior authorisation by Judges) (), in : *Il fatto quotidiano*, 18 June 2013, available at : http://www.ilfattoquotidiano.it/2013/06/18/datagate-allitaliana-monti-e-blitz-degli-007-sui-dati-senza-ok-della-magistratura/629830/.