Balancing the interests in the context of data retention (INVODAS)

Romania

Bogdan Manolea

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

Yes, the provisions of the Directive have been transposed in the national legislation by the Law on electronic communications data retention (Official title in Romanian : Lege nr.298 din 18 noiembrie 2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, precum şi pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private

în sectorul comunicaţiilor electronice) no 298/2008 published in the Official Monitor no 780 from 21.11. 2008.[1]

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. **What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?**

   N/A

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   N/A

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   N/A

- ***If transposition has been <u>accomplished</u>:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   There is no official translation of the text, but there is available an un-official translation of the law 298/2008 at the website of the Romanian Data Protection Authority – link – http://www.dataprotection.ro/servlet/ViewDocument?id=508

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   The law 298/2008 was published in the Romanian Official Monitor no 780 from 21.11. 2008. Article 23 para 1 specifically foresees that the law will enter into force in 60 days from its publication in the Official Monitor, therefore the date of entry into force was 20 January 2009.

---

[1] An electronic copy of the law can be found in Romanian at http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-2982008-privind-pastrarea-datelor-de-trafic-informational.html

According to Article 23 para 2:

”The provisions referring to the retain of traffic and location data relating to the Internet access, Internet e-mail and Internet telephony will be applicable starting with 15th of March 2009“

The law was in force until the Constitutional Court Decision 1258 from 8 October 2009 (published in the Romanian Official Monitor no. 789 of 23 November 2009.) when the law was considered unconstitutional.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc.)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

The Directive provisions were implemented by an ordinary Law. An Ordinary Law is a text adopted by the Parliament (formed by 2 chambers: Senate and Chambers of Deputies) by a majority of votes. For this law the deciding Chamber was the Chamber of Deputies. The Senate adopted the text on 17.06.2008 and the Chamber of Deputies on 4.11.2008.[2]

The law was initiated by the Government and registered at the Parliament on 20.02.2008. This is the standard procedure in the major part of laws adopted and almost in all cases when a Directive needs to be implemented.

The more technical-oriented decisions should have been included in an Order (called Norme metodologice, in practice a type of secondary legislation) issued by the Ministry of Communications and Information Technology (MCTI) according with article 22 of the adopted law:

"Within 30 days from entering into force, the Ministry of Communications and Information Technology shall elaborate the methodological norms for the application of the law and will submit them for approval to the Government. "

---

[2] See the file of the law at the Chamber of Deputies website - http://www.cdep.ro/pls/proiecte/upl_pck.proiect?cam=2&idp=9455

Even though the law foreseen a time-frame of 30 days from the date of entering into force, the deadline was never respected by the MCTI, who never issued the Order. A Draft Order was available on the MCTI website from 6.02.2009 for public consultation purposes, but the text was never adopted by the Ministry or the Government.

This is a normal procedure in cases when the Government wants to regulate highly technical issues. Not even the extra-time frame before passing a secondary legislation is not uncommon, although it is possible that the media reaction would have slowed down the process.

It is also worth mentioning that the Government announced several times in February 2009[3] that it will postpone the application of the law or it will "suspend"[4] it. The official reasons were related to the fact that the law is actually an obstacle for penal procedure and that the electronic communication operators are unable to cope with the law provisions on such a short deadline.

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?**

The terms defined in art 2. para 2 of the Directive are also defined in the Law 298/2008. The terms defined in the directive at Article 2 items a, b, c, d, e,f can be found almost identical in the Romanian Law Article 2 Para 1 items b, c, e, g, h, i.

Article 2 para 1 of the Directive is transposed almost identical in Article 2 Para 2 of the Romanian law, with a reference to the national law on implementing the Directive 95/46/EC (law 677/2001) and the Directives 2002/21/EC and 2002/58/EC (Law 506/2004).

Article 2 Para 2. Within the provisions of the law, the definitions provided by Article 3 of Law no. 677/2001, modified and amended, and the ones provided by Article 2 of Law no. 506/2004, modified and amended, are applicable.

The Romanian law also added some new definitions in Article 2 Para 1 items a, d, f and j:
„a)providers of electronic communications network and services – the person which provides, for commercial purpose, services and/or electronic communication networks to the end users or other providers of electronic communications network and services, in order to sustain their traffic;

---

[3] See official press release from the MCTI, 25.02.2009 - http://media.hotnews.ro/media_server1/document-2009-02-25-5447934-0-comunicat-mcsi.doc

[4] There is no such thing as „law suspension" in the Romanian legal framework.

(...)
d)subscriber – any legal entity or natural person which signed a contract with a provider of publicly available electronic communications network and services;
(...)
f)serious crime – crime which is part of the ones enumerated[5] at article 2 paragraph b) of Law no. 39/2003 concerning the prevention and suppression of organised crime, committed or not by an organised group, the ones provided[6] by chapter IV of Law no. 535/2004 concerning the prevention and suppression of terrorism and the ones against the state security provided by title I of the special part of Law no. 15/1968 – Criminal Code of Romania[7], republished, modified and amended;
(...)

---

[5] The list at article 2 paragraph b in law 39/2003 was at the time of law 289/2008 comprised by 20 crimes from the Penal Code or other penal laws, including any crime that was punished with at least 5 years inprosonment

1. omor, omor calificat, omor deosebit de grav;

2. lipsire de libertate în mod ilegal;

3. sclavie;

4. şantaj;

5. infracţiuni contra patrimoniului, care au produs consecinţe deosebit de grave;

6. infracţiuni privitoare la nerespectarea regimului armelor şi muniţiilor, materiilor explozive, materialelor nucleare sau al altor materii radioactive;

7. falsificare de monede sau de alte valori;

8. divulgarea secretului economic, concurenţa neloială, nerespectarea dispoziţiilor privind operaţii de import sau export, deturnarea de fonduri, nerespectarea dispoziţiilor privind importul de deşeuri şi reziduuri;

9. proxenetismul;

10. infracţiuni privind jocurile de noroc;

11. infracţiuni privind traficul de droguri sau precursori;

12. infracţiuni privind traficul de persoane şi infracţiuni în legătură cu traficul de persoane;

13. traficul de migranţi;

14. spălarea banilor;

15. infracţiuni de corupţie, infracţiunile asimilate acestora, precum şi infracţiunile în legătură directă cu infracţiunile de corupţie;

16. contrabanda;

17. bancruta frauduloasă;

18. infracţiuni săvârşite prin intermediul sistemelor şi reţelelor informatice sau de comunicaţii;

19. traficul de ţesuturi sau organe umane;

20. orice altă infracţiune pentru care legea prevede pedeapsa închisorii, al cărei minim special este de cel puţin 5 ani;

[6] Articles 32-39 from the Law 535/2004, as in force at the time of law 298/2008

[7] Articles 155-173 from the Romanian Penal code, as in force at the time of law 298/2008

j)unconnected call – a communication where a telephone call has not been technically finalised, meaning there was no connection between the calling person and the called person. „

Dimension 1 (State – citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

The data that have to be retained under Law 298/2008 were stipulated in art. 3-10 of the law and are identical to the ones prescribed by the Directive in Article 5 of the Directive. There are no additional retention obligations.

According with Article 10 of the Romanian law, the unsuccessful call attempts have to be retained, but not the unconnected calls. (see above definition of the latter)

(1) The providers of publicly available electronic communications services and of publicly communications networks, set up within Romanian jurisdiction, have the obligation to retain the data concerning the unsuccessful call attempts only where these data are generated or processed and store, as regards telephony data, or logged, as regards Internet data, within the activities of services providing.

(2) The providers do not have the obligation to retain the data provided by Article 3 paragraph (1) as regards the unconnected calls.

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

The Law on privacy in the electronic communications field (law 506/2004[8]) foresees in article 5 that the traffic data may be retained for billing and interconnection purposes, but after they are no longer needed, they need to be erased or made anonymous. Law 506 was preceding law on data retention 298/2009.

Article 5
Traffic data
Traffic data relating to subscribers and users, processed and stored by the provider of a public electronic communications network or by the provider of a publicly

[8] Published in Official Monitor no 1101 from 25.11.2004. An english translation is available here http://www.legi-internet.ro/english/romanian-itc-legislation-and-articles/date-cu-caracter-personal/romania-law-no5062004-on-the-processing-of-personal-data-and-the-protection-of-privacy-in-the-electronic-communications-sector.html

available electronic communications service, must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs (2), (3) and (5).
(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may only be processed up to the end of a period of 3 years from the due date of the corresponding payment obligation.
(3) For the purpose of marketing its electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph (1) only to the extent and for the duration necessary for such services or marketing, and only if the subscriber or user to whom the data relate has previously given his/her express consent. The subscriber or user shall be given the possibility to withdraw his/her consent for the processing of traffic data at any time.
(4) In the cases referred to in paragraphs (2) and (3), the provider of the publicly available electronic communications service must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing. In the case referred to in paragraph (3), this information must take place prior to obtaining the consent of the subscriber or user.
(5) Processing of traffic data, in accordance with paragraphs (1) to (4), may only be carried out by the persons acting under the authority of the providers of public electronic communications networks or publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing value added services, and is allowed only to the extent it is necessary for the fulfilment of these duties.
(6) Paragraphs (1) to (3) and (5) shall apply without prejudice to the possibility for competent bodies to have access to traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

The purpose of the law is foresee in article 1 of the Romanian law:
(1) The present law establishes the obligations of the providers of electronic communications network and services with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available to the competent authorities for the purpose of the investigation, detection and prosecution of serious crime.

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?**

There are several categories of sensitive data where the collection, interception or retention is prohibited, such as :

- There is a generic crime foreseen in the Penal Code (Art. 196 – Disclosure of the professional secret) that includes all types of disclosure that were prohibited by law:

Art.196 Disclosure of professional secrecy

The disclosure, without right, of data by the person to whom they were entrusted or which he/she learned, by virtue of profession or office, if the act is likely to cause prejudice to a person, shall be punished by imprisonment from 3 months to two years or by fine.
Criminal action in para. (1) is initiated upon prior complaint from the injured person. Reconciliation of parties removes criminal liability.

- the list of sensitive data from the Law 677/2001 on processing personal data – art. 7-11 (includes special articles on medical data and data regarding penal crimes);

- Law 51/1995 regarding the organisation and exerting the lawyer profession and the Bar Statues foresee the obligation of secrecy for all information received during a case. The documents at his office should be inviolable, as well as his telephony calls and professional correspondence, except in condition explicitly foreseen by law.

- The medical secrecy is regulated in a number of normative acts– Law 51/1994 on patient rights foresees in art 21-25 the confidentiality of the medical data related to a patient, Law 306/2004 which indicates keeping the professional secrecy (article 39 item h) as one of the obligations of the doctor, The Ethics Code of the Doctors (Art. 13-22 on Professional secrecy) or the Order of the Health Ministry no 240/2004 – Annex 1 (regarding privacy and secrecy in relation with Employment medical examination), etc.

- Various Ethical codes for Journalists that include the obligation to keep the professional secrecy and confidentiality of sources (e.g The main ethical

code is: The Ethic Code of the Journalist adopted by the Convention of Media Organisations on 9-11 July 2004.)[9]

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefore.**

According to Article 3 Para 2 of the Romanian law, the data needs to be retained for 6 months from the moment of the communication. No distinction is made on different categories.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

There are two categories of authorities that have the right to access the data:

a) Law enforcement authorities – with the procedure explained in articles 15-16.

b) "The state bodies with attributions preventing and counteracting the threats toward the national security " - mentioned in art 20 of the Romanian law "in the conditions established by normative acts which regulate the activity of national security "

It is very unclear what exact institutions would actually fit in the second category, as the text of the law is very vague – probably any security and intelligence authority in Romania.

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

The data retained may be used only in connection with investigation, detection and prosecution of serious crime. The list of serious crimes is mentioned in the definition of article 2. (see answer above to Q8)

There is no possibility to access the data retained under the current law in civil cases or in penal cases outside the list provided by the serious crimes definition.

---

9 See text in Romanian at http://crji.org/content.php?id=35&l=1

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

If the access is by the category b) , as described in point 14, the requirements are unclear – the text point to a legislation that can't be identified easily.

If the access is by the category a), as described in point 14, the requirements are established by the article 16 of the Romanian Law:

- if there are serious data or signs concerning the preparation or committing a serious crime, and
- If the criminal prosecution has began, and
- a motivated authorisation of the competent Court President or by the competent Prosecutor, only in emergency cases and only for a maximum 48 hours period after which it has to be approved by the competent Court President.

17. **Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?**

Yes, a motivated court authorisation of the competent Court President is required in order to access the data.

However, there is also an emergency procedure, when a competent Prosecutor might access the data for a maximum 48 hours period after which it has to be approved by the competent Court President.

It is not required to hear the aggrieved party or to to involve him/her otherwise in the proceedings before data is accessed.

18. **Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?**

There is no provision in the law 298/2008 regarding the notification of the aggrieved party of the data access.

However, there is such an obligation for notification in law 161/2003 art 57 para 4 in cases of intercepting and recording communications made by electronic communications means (this law implements the Council of European Cybercrime Convention text).

Also, there is a similar obligation for intercepting content communications foreseen in article 91^3 of the Penal Procedure Code.

But it can be argued that the two cases mentioned above are different in comparing with the blanket data retention (which contain no content communication), so the obligation of notification of data access does not apply to the case of law 298/2008.

19. **Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?**

    There is no provision in the law 298/2008 regarding the right of the aggrieved party to be informed about the data accessed.

20. **May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?**

    There is no provision in the law 298/2008 regarding the recourse of the aggrieved party for the data accessed. However, Article 1 para 4 mentions that:

    " The application of the provisions of the present law shall be done with the observance of the provisions of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, modified and amended, and of Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, modified and amended. „

    Therefore we may consider that the right to access its personal data, as foreseen by art 13 of the Law 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data, modified and amended also applies in this context.

    According to this text, the aggrieved party has the right to ask the competent authority or its electronic communication provider if his data was accessed by third parties. He also has the right to complain to the Data Protection Authority, if the competent authority or the electronic communication provider does not reply in due time.

    In case of unlawful data access or processing operation, the aggrieved party may ask for a penal investigation for a computer crime (e.g. illegal access to computer system – art 42 para 1 from law 161/2003 or Unauthorised transferring data from a computer system – art 44 para 2 law 161/2003) and may ask also civil damages during the penal trial.

21. **Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.**

    Yes, article 19 of the Romanian law 298/2008 foresees that

(1) Any intentional access or transfer of data stored according to the present law, without an authorization, constitutes a crime and is punished with imprisonment from one year to five years.

22. When do the accessing bodies have to destroy the data transmitted to them?

Destroying the data by the accessing bodies is regulated by art. 16 para 6-9 of the Law 298/2008.

Para 6 regulates the situation when the retained data not related to the fact that constitutes research object – the data is destroyed at the final solution of the case.

(6) The retained data not related to the fact that constitutes the research object are archived at the parquet's premises, in special places, in sealed envelope, by ensuring the confidentiality and can be communicated to the judge or, by request, to the group invested with finalising the cause. At the final solution of the cause, the date shall be deleted or, by case, destroyed by the prosecutor, by signing a minute.

Para 7 regulates the situation when the solution of not prosecuting was issued – the data is destroyed when the prescription term of the criminal responsibility for the action which constituted the cause is over.

(7) If the solution of not prosecuting was issued, the retained data are archived at the parquet's premises, in special places, in sealed envelope, by ensuring the confidentiality and are kept until the prescription term of the criminal responsibility for the action which constituted the cause is due, and when they are destroyed, a minute is signed.

Para 8 regulates the situation when the court declared a conviction, acquittal or cessation decision – the data is not destroyed and just archived.

(8) If the court declared a conviction, acquittal or cessation decision for the criminal process, which is definitive, the retained data are archived in the same time with the dossier at the court's premises, in special places, in sealed envelope, by ensuring the confidentiality.

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

The obligation to retain data is limited by Article 1 para 1 to the "providers of electronic communications network and services". The latter is defined in Article 2 Para 1 item a) as :

a) providers of electronic communications network and services – the person which provides, for commercial purpose, services and/or electronic communication

networks to the end users or other providers of electronic communications network and services, in order to sustain their traffic;

The definition is very close to the definition from Government Emergency Ordinance (OUG) no. 79/2002[10] on the general regulatory framework on communications – Article 2 para 1
provider of an electronic communications network – a person whose business consists, in whole or in part, of the provision of an electronic communications network;

The electronic communication network and the electronic communication service were already defined in the Government Ordinance 34/2002[11] on the access to the public electronic communications networks and to the associated infrastructure, as well as their interconnection in Article 2 item a) and b):

a) electronic communications network – the transmission systems and, where applicable, switching or routing equipment and any other resources which allow the conveyance of signals by wire, by radio, by optical or by other electromagnetic means,including satellite communications networks, fixed terrestrial networks, with circuit and package switching, and mobile, electrical networks – to the extent that they are used for the purpose of transmitting signals –, networks used for the broadcasting of the audiovisual programmes services, and cable television networks, irrespective of the type of information conveyed;

b) electronic communications service – a service, normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electroniccommunications networks, including telecommunications services and transmission services in networks used for broadcasting, but without including services providing, or exercising editorial control over, content of the information transmitted by means of the electronic communications networks or services; also, it does not include the information society services, defined under art.1 point 1 of Law no.365/2002 on electronic commerce, with the subsequent amendments and completions, which do not consist, wholly or mainly, in the conveyance of signals on electronic communications networks;

The interpreted definition thus excludes explicitly the information society service providers.

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g.

---

[10] A text of this law translated in English may be found on the ANCOM (Romanian Regulatory Authority on Electronic Communications) webpage http://www.ancom.org.ro/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/OUG_en79_2002.pdf

[11] A text of this law translated in English may be found on the ANCOM webpage http://www.ancom.org.ro/Portals/57ad7180-c5e7-49f5-b282-c6475cdb7ee7/OG%2034_2002_en.pdf

non-commercial service providers or service providers with a minor turnover/market share?

According to the interpretations above, the following groups were excluded by law:
- non-commercial service providers (this includes free WiFi hotspots in Cafes or Hotels)
- providers of electronic communications network and services to its own constituency (e.g. A network provider in a University)

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

It is very unclear what data categories have already been retained before the Directive entered into force, because there was never a study performed in this respect. This type of information is available only to law enforcement and electronic communication providers. Some information was gathered from these providers according with their declarations in the period of debate before the law 298/20008 was adopted.

It seems though that in case of the Internet-related services very little data or even no data (in case of the small and medium ISPs that offered an unlimited Internet access) was kept.

In the case of telephony providers, most of the data covered by the directive was already kept by the fixed and mobile telephony operators for billing and interconnection purposes. (except data necessary to identify users' communication equipment or what purports to be their equipment and data necessary to identify the location of mobile communication equipement.)

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

According with Article 12 of the Law 298/2008, there were established some principles for data security of the data retention:

The activity of data retention is carried out by observing the following principles:
a)the retained data shall be of the same quality and subject to the same security and protection as those data on the network;
b)the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
c)the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only.

These should have been detailed in the secondary legislation, that was in fact never adopted, as explained above.
Also, the reference to Law 506/2004 regarding the protection of privacy in the field of electronic communications and to Law 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data also mean that the electronic communication providers are bound by the data security obligations already adopted in this field:

- Article 3 Security Measures from Law 506/2004[12]

(1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its service. With respect to network security, if necessary, the provider of the publicly available electronic communications service shall take those security measures in conjunction with the provider of the public electronic communications network. Having regard to the state of the art and the cost of their implementation, the measures taken shall ensure a level of security appropriate to the risk presented.
(2) The National Regulatory Authority for Communications shall establish the conditions under which the providers must fulfil the obligation set out in paragraph (1).
(3) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must:
a) inform the subscribers of such risk and of the possible consequences ensuing;
b) inform the subscribers of any possible remedies;
c) inform the subscribers of the likely costs involved by eliminating the risk.

Please note that the conditions on security foreseen in Para 2 were never established by the Regulatory Authority in Communications (now titled ANCOM)

- Order of the People's Ombudsman (former Romanian Data Protection Authority) no 52/2002 [13] - Minimal security obligations for processing personal data. This was the secondary legislation for the application of article 20 para 2 of the Law 677/2001 on data protection.

---

[12] An english translation of this law is available at http://www.legi-internet.ro/english/romanian-itc-legislation-and-articles/date-cu-caracter-personal/romania-law-no5062004-on-the-processing-of-personal-data-and-the-protection-of-privacy-in-the-electronic-communications-sector.html

[13] Text available only in Romanian at http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/ordinul-522002-privind-aprobarea-cerintelor-minime-de-securitate-a-prelucrarilor-de-date-cu-caracter-personal.html

27. **Which additional costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?**

    It is impossible to estimate the additional costs from the implementation of the national law transposing the Directive in Romania. Such a study was never made or even estimated by the Government or private sector.

28. **Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?**

    No, the obligated parties do not receive any reimbursement for their costs by the Government.

29. **What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?**

    There are no specific rules that govern the cooperation between electronic communication providers and law enforcement authorities. There have been a number of attempts to create a Protocol between the two parties, but no final document is sign.

    Besides this, there are generic provisions that oblige any citizen to cooperate in good faith with the law enforcement authorities for crime prosecution.

30. **Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.**

    Article 19 of the law 298/2008 foresees two crimes in relation with the infringement of the law provisions:

    (1)Any intentional access or transfer of data stored according to the present law, without an authorization, constitutes a crime and is punished with imprisonment from one year to five years.
    (2)The intentional obstruction of communicating the retained data to the competent authorities, as a consequence of applying the present law constitutes a crime and is punished with imprisonment from 6 months to one year.
    (3)The attempt to the infringement provided by paragraph (1) is punished.

Also, other crimes may be retained [committed?yes] (e.g. illegal computer data transfer) depending on the specific case. In all cases the damaged party may ask for moral or material damages.

Also Article 18 of the law 298/2008 establishes contraventions for

- retaining the data less than 6 months (item a of Article 18)
- retaining more data than prescribed by law or not deleting the data after 6 months (item b of Article 18)
- not respecting the data retention principles in Article 12 (see above Q26) – item c of Article 18.

The contraventions may be applied by the Data Protection Authority and the fine is between 2500 – 500 000 RON (approx. 600 – 119 000 Euros)
According to the Civil Code law provisions, in all cases the damaged party may ask for moral or material damages in a separate civil action.

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

There is no specific public body responsible for establishing the contact with the party retaining the data. Therefore the body that may access the data needs to establish the contact.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

There are no regional entities vested with own authority that have been granted their own rights of access.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

There are different types of generic rules of co-operation between different public authorities, depending on the topic of the crime. For example:

- Law 14/1992 regarding the functioning of the Romanian Intelligence Service (SRI) established the general framework of cooperation with the Law enforcement authorities (especially Prosecutor's Office). There are also

additional Protocols with other law enforcement institutions (such as the Anti-corruption National Prosecutors' Office)

- Law 656/2002 on the prevention and sanctioning of money laundering which establishes the cooperation between The National Office for Prevention and Control of Money Laundering and the law enforcement authorities.

- Emergency Ordinance 91/2003 regarding the functioning of the Financial Guard – establishes the cooperation on investigation of financial crimes between the Financial Guard and the law enforcement authorities.

The general rules of co-operation haven't been updated in the course of the Directive's transposition.

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

According with the law 161/2003 (that implemented the provisions of the CoE Cybercrime Convention) Article 60 – the Romanian judicial authorities are cooperating with similar authorities from other states, in the conditions established by international treatise and national Laws.

Article 62 establishes the Service of Combating Cybercrime from the Prosecutor's Office attached to the Supreme Court of Justice – Organized Crime Section as a permanent contact point that may ask for data conservation, including the retention of the objects that contain traffic data that are requested by a foreign competent party.

Article 63 is detailing the procedure to ask for the data conservation and the decision is valid until a Romanian court has issued a decision on the request of international legal assistance for penal matters from the foreign authority.

The national authorities responsible for the cross-border data exchange in cases of cybercrime are established by the Law 64/2004[14] for ratification of the Council of Europe Cybercrime Convention – Article 1 Para 2 item b)

b) According to article 17 Para 2 item c from the Convention:

The central authorities designated to transmit and receive the requests of judicial assistance are:

---

[14] Published in the Official Monitor of Romania no. 343 from 20/04/2004

- Prosecutor's Office attached to the High Court of Cassation and Justice for the requests of judicial assistance formulated during the penal investigation

- The Ministry of Justice or the requests of judicial assistance formulated during the trial or execution of the punishment.

At the same time we need to underline that the law 298/2008 did not foresee any specific obligation of exchanged the data with other law enforcement authorities.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

According to article 17 of the Law 298/2008 the competent authority to monitor the application of the provisions of the present law is the National Supervisory Authority for the Processing of Personal Data (the Romanian Data Protection Authority). Also Article 18 para 3 gave the authority to power to establish the contraventions and apply sanctions, including on the data security principles.

The supervision is limited to the contraventions established in Article 18 of the Law 298/2008 and the ones in the Law 677/2001 regarding the processing of personal data, therefore is more a control of legality of protecting personal data (including technical advisability), but not on the legality of the each access to the data.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

c) **Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?**

There was one lawsuit initiated by an NGO – Comisariatul pentru Societatea Civila (Civil Society Commissariat) against its mobile telephony operator – Orange Romania – case no. 2971/3/2009 at the Bucharest Tribunal. The case documents are not publicly available, but according to declarations by the plaintiff, the case was initiated to ask the telephony operator, via an interim measure called Presidential Ordinance, not to retain the traffic data of his communication and to respect the contractual obligations regarding the confidentiality of the communications

The case was mainly used to raise an unconstitutionality exception in one of the hearings, so that the case could be reffered to the Romanian Constututional Court. This case was closed after the favorable decision of the Romanian Constututional Court that considered the law unconstitutional. (see below)

There might have been also other cases as well, but they were not publicly presented.

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

No

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

There were no provisions in any normative act on this subject, therefore the data was stored at the service providers' premises – locally. Apparently the secondary legislation should have clarified this aspect.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

According to the framework law on data protection 677/2001, these data can be transferred abroad only in the conditions of Chapter VII – only if the recipient state has an adequate level of protection.

There were no provisions in Law 298/2008 on this subject.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

This is a contravention according to Article 18 Para 1 Item b. Other organisational measures should have been adopted by the secondary legislation, which was not in place.

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)?

No measure in practice. Other organisational measures, such as an automatic system to log any access to the data, should have been adopted by the secondary legislation, which was not in place.

However, this is a crime according to Art 19 Para. 1

Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

There were no technical interfaces enabling State bodies to access the data directly.

c) data are not used for purposes other than those they are permitted to be used?

No measure in practice. Other organisational measures should have been adopted by the secondary legislation, which was not in place.

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

No real measure in practice.

Non-observance of the principles of data security in Article 12 is a contravention.

Other organisational measures should have been adopted by the secondary legislation, which was not in place.

e) **data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?**

No real measure in practice.

Non-observance of the principles of automatic deleting the data after the retention period has passed in Article 11 para 3 is a contravention.

Other organisational measures should have been adopted by the secondary legislation, which was not in place.

f) **the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?**

There is no such provision in law 298/2008. See also answer to Q19

g) **sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?**

No real measure in practice.

41. **Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?**

No, there was no effective control that the measures will be applied.

42. **What technical (de facto and/or de iure) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?**

These standards should have been detailed by the secondary legislation, which was not in place. De jure we can make only reference to the Order of the People's Ombudsman (former Romanian Data Protection Authority) no 52/2002 [15] - Minimal security obligations for processing personal data.

However, de facto, it seems that these standards were not really respected especially by small and medium electronic communications providers.

For the period when law was applied, each provider designed its own system, without an interoperability obligation or taking into consideration security standards.

---

[15] Text available only in Romanian at http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/ordinul-522002-privind-aprobarea-cerintelor-minime-de-securitate-a-prelucrarilor-de-date-cu-caracter-personal.html

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

There was no standard procedure for the data transmission. This was part of the objective of the secondary legislation, which was never adopted.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

There was no provision in this respect.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

Generally, the Romanian society is not too interested in the measures of public surveillance. Or – better said some time not interested at all (such as cases on DNA Database law, CCTVs, PNR of Swift Agreement) and sometime overreacting with arguments of all sorts, but not related with human rights (such as passports and data retention law). [16]

There is still a general tendency to be really cautious will all kind of communication interceptions, maybe also as a follow-up of the Communist times when phone tapping and surveillance was a regular activity of the Securitate, former communist secret service. Actually even today a lot of people think that their phone is tapped (legally or illegally). Cases of people retained for corruption acts that are proven by (legally) intercepted phone calls are quite common. Almost always the phone taps transcriptions leak to the press from the Prosecutor's file in just a couple of days after an arrest.

---

[16] A more generic image in the beginning of 2009 can be found in this article written by Bogdan Manolea, EDRi-gram 7.2, 28.01.2009 - Romania: Is really privacy a topic in the public debate? available at http://www.edri.org/edri-gram/number7.2/romania-privacy-in-public-debate

There are in fact mainly two poles of interest in privacy and public surveillance issues in the society:

- one is by the human rights civil society. There are a few NGOs – APADOR-CH, Activewatch, Public Policies Institute or APTI (the latter more focused in digital rights) that are active in this domains.

- The second one is some (sometimes conservatory) Orthodox groups, that believe that the public surveillance is becoming generic and this is a direct attack towards their Orthodox Christian faith. Using theological arguments to present their case, they have a much bigger media presence, good activists in getting people involved, but sometime use irrational arguments (such as the presence of the number 666 in all biometric passports, which mean that the Devil is present in these acts)[17]. The groups have become more organized from the beginning of 2009, gathered in the "Coalition against the Police State"[18] The Patrarchy of the Orthodox Church have rejected the opinions of those groups, at least in the case of the biometric passport.

As regards the data retention, there was no reaction from the Romanian media and society when the EU Directive on data retention was passed. Only APTI supported the European Campaign organized by EDRi- Data retention is no solution.[19]

The public debate strated officially in April 2007[20] when the Minsitry of Information Technology and Communications issued a first draft and organized a public debate arround it. They received some complaints from civil society groups and ISPs Association, but this was a fairly quite event.

Nothing happend for almost one year, when the Minsitry was reminded about the law, so a similar version to the one presented in April 2007 was adopted by the Government in February 2008 and sent to the Parliament for discussions. This also went almost un-noticed by the general public. The path of the law through the two chambers of the Parliament went smooth, without major amendments (except reducing the retention period from 12 months to 6 months)[21]

A public debate organized by APTI together with the Council of Europe Information Office in Bucharest on 6.03.2008 received just a very limited attention – mainly from ISPs, civil society groups and one journalist. Even the repesentative of the Minsitry that attended called it an inefficial and useless law.

---

17 See also EDRi-gram 7.3 - Bogdan Manolea - Romania: Protests against biometric passports – 11.02.2009 http://www.edri.org/edri-gram/number7.3/romania-biometric-passports-protests

18 Information at the (only in Romanian) http://www.curaj.net/?p=9530

19 More info available at http://www.dataretentionisnosolution.com/

20 See info in EDRi-gram 5.9. Bogdan Manolea - First draft on data retention law in Romania 9.05.2007 - http://www.edri.org/edrigram/number5.9/data-retention-romania

21 See EDRi-gram 6.4 , Bogdan Manolea - Romanian Govt adopts Data retention law, but calls it inefficient , 27.02.2008 http://www.edri.org/edrigram/number6.4/romania-data-retention

The parcourse of the law in the Parliament was not significant. In the Senate the law received the positive approval from the Human Rights Comitte[22] and the law was adopted with no votes against and just 2 absentions. In the Chamber of Deputies the law received a Negtive advice from the Human Rights Committe[23], but a Positive one from the Legal Committe and IT&C Comittee[24], who were the deciding committees for this law. The final text was adopted by the Chamber of Deputies with no votes against and 1 abstention.[25]

The law 298/2008 was then promulgated by the President and published in the Official Monitor.

The overall reaction to the law change dramatically in January 2009 when the law was scheduled to enter into force. Suddenly and without a possible easy explanation, all media starting discussing about the new law that will keep the traffic data (and in a lot of articles it was said that also the content of communication will be kept) and the pro-orthodox groups became active in criticizing the law and its outcomes. Also politicians started saying that the law is bad and needs ti be repealed.

Several civil society groups asked the Romanian Ombudsman to promote an action to the Constitutional Court to check for its constitutionality, but the Ombudsman claimed on 10.02.2009 that the law is constitutional, so the action is useless.[26]

Getting unsatisfactory comments also from the law enforcement authorities (that said the law was not flexible enough), the Government announced that it will „suspend“ the law. This calmed the spirits a little bit, even though the law was never „suspended“.

The professional associations, labour unions, consumer and business organisations were never involed in discussions on this topic (except for the ISP Associations that were there all the time)

The Data Protection Authority was quite during all the debates. (in fact the Romania Authority sees its duties only in connection with law 677/2001 on personal data protection and nothing more).

The law enforcement agencies were not at all asking for the data retention act, but starting complaining after the act was passed, that it has limit their action. The law 298/2008 allowed the access to the data only if a penal action was started, while

---

22 Text available at http://webapp.senat.ro/pdf/08L166CA.pdf

23 Text available at http://www.cdep.ro/comisii/drepturile_omului/pdf/2008/av439.pdf

24 Text available at http://www.cdep.ro/comisii/juridica/pdf/2008/rp439.pdf

25 Text of the „debate“ in teh Chamber of deputies available at http://www.cdep.ro/pls/steno/steno.stenograma?ids=6558&idm=8

26 See info at http://www.ziare.com/ccr/avocatul-poporului/avocatul-poporului-nu-va-sesiza-ccr-cu-privire-la-legea-interceptarilor-668636

according to the Penal Procedure Code they could do wiretapping (with a judicial approval) even when they didn't reach this stage.

The officials os MCTI seemed really unhappy with the law, but claimed that they had no other choice since it is an obligation according to EU laws. Same attitude was made by the President of the IT&C Committe in the Chamber of Deputies, Mr. Varujan Pambuccian, who said that is a useless law, but had to be passsed.

46. Are there any obligations in your country to retain other personal data without a *specific* reason (e.g. passenger name records (PNRs), employment data, etc)?

According with the law 677/2001 on processing personal data, there shouldn't be an obligation to retain personal data without a specific reason. However the law 677/2001 does not apply to public defence or national security domains.

Also, Romania – as part of the EU – is covered by the US-EU PNR agreement and other PNR agreement concluded by the EU.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

For the time when the law was in force, there were no statistics available regarding its application.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

Same as above, not available.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

After the Decision of the Constitutional Court, the law is not in force anymore therefor this question is not applicable.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of

profession in cases where the confidentiality of communication is essential etc.)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law27 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The Romanian Constitution[28] adopted in 1991 recognizes under Title II (Fundamental Rights, Freedoms and Duties) the rights of privacy, inviolability of domicile, freedom of conscience and expression. Article 26 of the Constitution states, "(1) Public authorities shall respect and protect the intimate, family and private life. (2) Any natural person has the right to freely dispose of himself unless by this he causes an infringement upon the rights and freedoms of others, on public order or morals." Article 27 states, "(1) The domicile and the residence are inviolable. No one may enter or remain in the domicile or residence of a person without consent. (2) Derogation from provisions under paragraph (1) is permissible by law, in the following circumstances: for carrying into execution a warrant for arrest or a court sentence; to remove any danger against the life, physical integrity or assets of a person; to defend national security or public order; to prevent the spread of an epidemic. (3) Searches may be ordered only by a magistrate and carried out exclusively under observance of the legal procedure. (4) Searches at night time shall be prohibited, except in cases of flagrante delicto." Article 28 states, "Secrecy of the letters, telegrams and other postal communications, of telephone conversations and of any other legal means of communication is inviolable." According to Article 30, "(6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of person, and the right to one's own image."

Also, the Article 1 Para 3 of the Constitution mentioned the"free development of human personality" that is a guaranteed supreme value:

(3) Romania is a democratic and social state, governed by the rule of law, in which human dignity, the citizens' rights and freedoms, the free development of human personality, justice and political pluralism represent supreme values, in the spirit of the democratic traditions of the Romanian people and the ideals of the Revolution of December 1989, and shall be guaranteed.

As regards the scope of these fundamental rights as established by the Romanian Constitution, these are difficult to asses in the lack of relevant decisions on the relevant articles mentioned above that may picture the jurisprudence of the Romanian Court.

---

27 In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

28 Text in english at the Chamber of Deputies website http://www.cdep.ro/pls/dic/site.page?id=371

The first case dealing with the secrecy of communication was the decision 1258 from 8 October 2009[29] regarding the unconstitutionality of the law 289/2008.

In this case the Constitutional Court explains that the traffic data is related to the private life and its blanket retention may prejudice the freedom of expression of right of communications:

"The Constitutional Court observes that, even though Law 298/2008 refers to data with a predominantly technical character, these are retained with the scope of providing information regarding a person and its private life.Even though according to art 1 para 3 of the law this does not apply to the content of the communication or to information accessed while using an electronic communication network, all the other retained data with the scope to identify the caller and of the called party, namely the user and the recipient of an information sent by an electronic way, the source, the destination, the date, the hour and length of a communication, the type of communication, the communication equipment or the devices used by the user, the location of the mobile communication equipment, as well as other „related data" - not defined in the law – are likely to prejudice, to inhibit the free usage of the right to communication or to expression."

As regards the scope of the retention, the Court also notes that without a proper defined scope of the Law 298/2008, the limitation of individual rights can't respect the limits established by Constitution and the European Convention on Human Rights:

„Without taking the place of a legislator, the Constitutional Court observes that the accurate regulation of the scope of law 298/2008 is more necessary considering especially the complex nature of the rights that are subject to limitations, as well as the consequences that a possible abuse of the public authorities might have on the private life of the subjects, as it is understood at the subjective level of each individual."

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The generic limitation of exercise of the fundamental rights it is permited in the limits established by Article 53 of the Constitution

(1) The exercise of certain rights or freedoms may be restricted only by law, and only if absolutely unavoidable, as the case may be, for: the defence of national security, public order, health or morals, of the citizens' rights and freedoms; as required for conducting a criminal investigation; for the prevention of the consequences of a natural calamity or extremely grave disaster.

---

[29] An unofficial English translation is available here http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

(2) The restriction shall be proportional to the extent of the situation that determined it and may not infringe upon the existence of the respective right or freedom.

Other specific limitations are prescribed by the Constitution as for example:

- in case of the right to privacy, Article 26 para 2 foresees

”Any natural person has the right to freely dispose of himself unless by this he causes an infringement upon the rights and freedoms of others, on public order or morals.“

- in case of Freedom of Expression – Article 30 Para 5-8

(5) The law may impose upon the mass media the obligation to make public their financing source.
(6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of person, and the right to one's own image.
(7) Any defamation of the country and the nation, any instigation to a war of aggression, to national, racial, class or religious hatred, any incitement to discrimination, territorial separatism, or public violence, as well as any obscene conduct contrary to morality shall be prohibited by law.
(8) Civil liability for any information or creation made public falls upon the publisher or producer, the author, the producer of the artistic performance, the owner of the copying facilities, radio or television station, under the terms laid down by law. Indictable offences of the press shall be established by law.

The limitations can also be prescribed by the international conventions where Romanian is a signatory or ECHR jurisprudence.

Other limitations can be explained through the jurisprudence of the Constitutional Court. Even in the case mentioned above the Court notes that

„ (...) the individual rights cannot be exercised in absurdum, but can constitute the object of restrictions, that are justified in connection with the desired scope. The limitation of the exercise of certain personal rights by considering collective rights and public interests that are related to national security, public order or penal prevention, has always been a sensitive operation from the regulation point of view, so that a fair balance may be achieved between individual rights and interests, on the one hand, and the rights and interests of society, on the other hand. It is also true, as the ECHR has remarked in the case Klass and others vs Germany, 1978, that taking surveillance measures without adequate and sufficient safeguards can lead to„destroying democracy on the ground of defending it ." „

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

Yes, the Constitutional Court has rules through decision1258/2009 that the Law 298/2008 in its entirety is unconstitutional.

The court did not directly addressed the subject of possibility to transpose the Directive in the national law by respecting constitutional framework, but left some possibility for that by considering in its decision:

" The legal regime of such a Community act foresees the obligation for the European Union member states related to the legal solution covered, but not to the concrete modalities on how the scope is being reached, the states enjoying a wide margin of solutions to adapt those regulations to the specificity of the legislation and national realities. "

At the same time, in the case for the law 298/2008 the Court seems quite clear that an obligation to retain all the data would be contrary to the present Constitution:

"(...)law 298/2008 imposes the obligation of a continuous retention of traffic data, from the moment of its entry into force and its application (...) without considering the necessity for the cessation of the limitation once the determinant cause has disappeared. The intrusion into the free exercise of the right takes place continuously and independently of the occurrence of a justifying fact, of a determinant cause and only for the scope of criminal prevention and the discovery – after their perpetration – of serious crimes."

and

"The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008, is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, but rather the legal obligation with a continuous character, generally applicable, of data retention. This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. Law 298/2008, even though it uses notions and procedures specific to the penal law, has a large applicability – practically to all physical and legal persons users of electronic communication services or public communication networks - so, it can't be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression. "

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

The Constitutional Court jurisprudence can't establish an absolute limit as regards the maximum degree to which public surveillance measures collectively may restrict fundamental rights. This is made on a case-by-case basis taking into consideration each case and the text of article 52 mentioned above.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

The Constitutional Court did not rule on specific exemptions, but noted that the retention all data "is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes."

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

The Constitutional Court already ruled on Law 298/2008 and consider it unconstitutional.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

There was no provision in the Law 298/2008 regarding the conditions or the limits imposed to the electronic communication providers that were obliged to retain the traffic data.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

No.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

According to article 20 of the Romanian Constitution on International treaties on human rights, the Constitutional provisions concerning the citizens' rights and liberties shall be interpreted and enforced in conformity with the International treaties where Romania is a party to.

Also if there are any inconsistencies exist between the conventions and treaties on the fundamental human rights Romania is a party to, and the national laws, the international regulations shall take precedence, unless the Constitution or national laws comprise more favourable provisions.

As the ECHR fits into the category on international human rights treaties, it results that the Convention takes precedence, unless Romania has national regulations more favourable.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

According to article 148 of the Constitution Para 2. "the provisions of the constituent treaties of the European Union, as well as the other mandatory community regulations shall take precedence over the opposite provisions of the national laws, in compliance with the provisions of the accession act. "

As regards the directives, since they are not directly applicable in the national legislation, they need to be transposed via national normative acts. However, this does not preclude the direct effect of directive, in conditions established by the ECJ in its jurisprudence.

The regular steps that are taken for a national implementation of a directive are: First draft established by the Government (usually by one of more Ministries – this includes a period of public consultation), Draft Adopted by the Government and send to the Parliament. Both of the Chambers of Parliament will discuss the text and adopted it.(one will be the deciding chamber - for details see article 75 of the Romanian Constitution)

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

No, there is no article foreseeing the transfer of national sovereignty to the European Union or the conflict between the Constitution and EU competences

There is no specific Constitutional limit to the transfer is such powers. See below article 148 of the Romanian Constitution, which deals with relations betwene EU Treaties and national legislation.

Article 148 Integration into the European Union

(1) Romania's accession to the constituent treaties of the European Union, with a view to transferring certain powers to community institutions, as well as to exercising in common with the other member states the abilities stipulated in such treaties, shall be carried out by means of a law adopted in the joint session of the Chamber of Deputies and the Senate, with a majority of two thirds of the number of deputies and senators.

(2) As a result of the accession, the provisions of the constituent treaties of the European Union, as well as the other mandatory community regulations shall take precedence over the opposite provisions of the national laws, in compliance with the provisions of the accession act.

(3) The provisions of paragraphs (1) and (2) shall also apply accordingly for the accession to the acts revising the constituent treaties of the European Union.

(4) The Parliament, the President of Romania, the Government, and the judicial authority shall guarantee that the obligations resulting from the accession act and the provisions of paragraph (2) are implemented.

(5) The Government shall send to the two Chambers of the Parliament the draft mandatory acts before they are submitted to the European Union institutions for approval."

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

Romania is not a federal state, so this is not the case – no regional entities dealing with powers on data retention.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

No.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

Now, the situation is quite clear with the data retention law being considered unconstitutional.

However, it is unclear what will be the future reaction of the Romanian Government. So far, almost one year after the Constitutional Court decision there has been not public reaction at all in any direction.

The improvement will be for the Romanian Government to assess the current Constitutional Court decision and to act accordingly at the EU level and to ask at the review of the data retention directive either for the repeal of the directive – or make the obligation optional for EU member countries.

Balancing the interests in the context of data retention (INVODAS)

Romania

Bogdan Manolea

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

No, there is no legislation that provides this right.

2. Please illustrate in detail any amendments to current (i.e., in the case of Romania, supposedly non-existent any more) data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

There are presently almost no discussions of the former data retention law in Romania. The only notable action was the open letter1 released in January 2011 by 10 NGOs (at the initiative of ApTI, which is the organisation where I work) that was not answered by any Romanian MEP. (it was send to all Romanian MEPs and to the Commission). Also, it wasn't picked up by the Romanian media.

As regards reactions from the Romanian authorities, officially there is almost none.

[1] http://www.apti.ro/pastrare-date-trafic.pdf

The only reaction was made in Brussels at the 3rd December 2010 data retention conference from a Romanian representative of the Ministry of Justice[2]that let the audience to understand that it would be impossible for Romania to implement the data retention law after the Constitutional Court Decision.

However, this was never discussed publicly in Bucharest.

From an unofficial source, we found out a rumour that the Ministry of Communications and Information Society will try to suggest a new data retention law (the first draft was initiated by Ministry of Justice), however nothing was made public so far.

Not even the review of the data retention directive did not attract any relevant attention from the press (besides copying the Commission's press release).

As regards art 16 para2 from the CoE Cybercrime convention, this is already implemented since 2003 by law 161/2003 Title III on cybercrime in Article 543 and following:

Procedural provisions
Art.54 - (1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be disposed.
(2) During the criminal investigation, the preservation is disposed by the prosecutor by a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court settlement.
(3) The measure referred to at paragraph (1) is disposed over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

3. In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means other than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?

All citizens or undertakings have the obligation to cooperate to the fullest extent possible to the law enforcement for crime detection, investigation and prosecution – this is a principle in the penal law and penal procedure law. However, there are only indirect means that fulfil this obligation.

---

2 Alina Barbu, Chief of Service, Romanian Ministry of Justice https://www.bof.nl/live/wp-content/uploads/295871-Report-conference-DRD-3-December-2010-1.pdf

3 Cybercrime provisions in law 161/2003 available at http://www.legi-internet.ro/english/romanian-itc-legislation-and-articles/criminalitate-informatica/romanian-cybercrime-law.html

Thus a person can be accused of false testimony[4] in any case that doesn't concern him as a defendant. It is considered a crime if a witness makes false testimony in a penal, civil or disciplinary case or withholds anything in relation with essential information on what he was asked about. This includes providing any data or documents related to the specific case.

Other crime that could be applicable might be to favour the lawbreaker[5], without any agreement, in order to complicate or defeat the penal investigation, prosecution or execution or in order to get the product of the crime to the lawbreaker. In some cases it might also be applicable a crime relate to conceal goods as a crime product.[6]

There exists also an obligation to inform authorities in case of any information regarding the commitment of specific serious crimes (burglary, homicide, etc.[7]) or if the crime known by a public servant in relation with his work-related duties.[8]

The new penal code adopted in 2009 (but not yet in force)[9] includes a much more specific article, making a crime obstructing the justice.[10] This article includes that it is considered a crime to refuse to present to the law enforcement authorities all or part of the data, information, documents or goods, that have been explicitly requested, based on the law, for solving a case.

An undertaking is also obliged to respect the obligations from the Penal Code. Chapter IV[1] indicates the amount of the fines that the undertaking might need to pay in case of breach of these crimes. In most of the cases it could be that also the manager of the undertaking could be responsible under the penal law as a natural personal as well.

As regards the extent, the current texts do not provide any specific limitations and, as far as we are aware, there haven't been any discussions in the doctrine in this respect.

4. Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive

---

4 Art 260 Penal Code

5 Art 264 Penal Code

6 Art 221 Penal Code

7 Listed in Art 262 Penal Code

8 Art 263 Penal Code

9 Law 286/2009 regarding the Penal Code, published in Official Journal no 510 from 24.7.2009. The law for the application of the Penal Code was adopted by the Senate and is now in discussions in the Chamber of Deputies. This law foresees as the date of application 1 October 2011.

10 Article 271 New Penal Code

2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?

Note – I guess the first question refers to situations to refuse to testify against other people, not against themselves. You could never be punished for refusing to testify or deliver evidence against yourself.

There are a series of professionals that have confidentiality obligations according to the law, their professional statutes or ethics. This includes lawyers, doctors, pharmacists, priests or even other activities that has this obligation (such as a banking employee).

If these persons are breaching their confidentiality obligation and this causes damage to the client, it could be a crime under art. 196 Penal Code Divulging Professional Secrecy. This crime can be performed also by omission (for example not protecting the secret information you have access to) and can be committed only with intent (thus not by mistake). Also the breach must be *without right*. This means the crime is not committed that in the case when the law obliges the person to inform the authorities (see art 262 Penal Code[11]).

Also, the Penal Procedural Code establishes that[12] a personal that is obliged to keep the processional secrecy can't be heard as a witness as regards the facts or circumstances regarding the profession. The only exception is obtaining the consent of the concerned person.

As regards the connection with the data retention law, this might occur only when the legal or physical person retaining the data has a confidentiality obligation towards the subject data. As the law is obligatory only for electronic communication providers, this situation might not occur at all.

Thus even though the electronic communication providers have a confidentiality obligation according to law 506/2004 (implementing the e-privacy directive), the data retention law modified law 506/2004, so this retention would be an accepted exception. (*with right*)

The law does not foresee the situation when a third party (such as the electronic communication provider) would interfere with this obligation of confidentiality. Of course this should be seen as a breach of the secrecy of correspondence if made without right.

But the obligation of confidentiality is on the persons from specific professions (doctor, lawyer, etc.), so knowing that data of all citizens are retained and if these data are covered by the confidentiality obligation (such as the case when a

11 See supra fn 7

12 Article 79 para 1

psychologist calls its patient), these persons can take all the technical measures (e.g. encryption) to be sure that the confidentiality is respected.

5. **Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?**

   There were no provisions in place in this respect when the law was in place. This should have been the details for the secondary legislation, which was never adopted, as explained in the first answer.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

   No

B. Country-specific questions

7. **Please give your own opinion on the constitutionality of the data retention regime in your country *as a whole*.**

   Our opinion is concurring with the one clearly established by the Constitutional Court: Any data retention regime with an obligation of retention of personal data, with a continuous character, applicable to all law subjects is unconstitutional.

8. **Are the data to be retained in accordance with the Directive covered by the secrecy of correspondence, as provided for by the national (constitutional) law of your country?**

   The Constitutional Court has clearly ruled in the data retention case13 that the traffic data is personal information:

   "The Constitutional Court observes that, even though Law 298/2008 refers to data with a predominantly technical character, these are retained with the scope of providing information regarding a person and its private life."

   Also according with the ECtHR jurisprudence (see case Copland vs UK), these data are part of the communication:

   The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the

[13] Text at http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

communications made by telephone" (see Malone v. the United Kingdom, judgement of 2 August 1984, Series A no. 82, § 84).

The Romanian court has also considered that the law on retained data breaches the secrecy of correspondence right as foreseen in the Constitution. (Art 28)

The data retention law "can't be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression."

9. **Please answer to the following questions with regard to the Constitutional Court's ruling on the constitutionality of data retention (see your answer to question 52 of the first questionnaire):**

   - **Does the deciding court provide any specific elements that have to be considered, or certain aspects that have to be balanced against each other when assessing whether or not the national law transposing the Directive is in line with the Constitution and other overriding law?**

     No, but that is because the Constitutional Court jurisprudence is considered not to create any legal provisions (positive law), so the Court usually refrains from suggestions on how the law should be changed in order to be considered constitutional.

     The reference to art 91^1 from the Penal Procedure Code on audio and video interceptions and recording (that were ruled constitutional) is a specific element that can be considered in co-relation with the data retention. The court notes that the Penal Procedure Code provides these audio and video interceptions as strict an exception, only in specific cases and only for maximum 120 days. Then the court notes:

     "Contrary, Law 298/2008 foresees as a rule what the Penal Procedure Code has regulated as a strict exception and obliges the permanent data for a 6 month period from its interception."

     So the main elements considered to be unconstitutional were the continuous character of the retention and their application to all citizens (by default, without a judge decision)

   - **To the court's opinion, is it possible to introduce a national law that is in line with both the fundamental rights enshrined in the Constitution/the human rights as laid down in the ECHR on the one hand and the provisions of the Directive on the other hand?**

     The Constitutional Court seems to note that such a national law might be adopted in order to fulfil with the Directive and ECHR *(see text quoted below).*

However, we believe that the Court knew very well that they can't rule the unconstitutionality of the Directive as such or to directly claim that the directive would be impossible to be implemented in Romania.

Thus the decision includes a rather vague text that can interpreted that such data retention provisions could be implemented, but at the same time strikes down the entire law as unconstitutional. The text is clear that the scope of the directive and of the Romanian law (retaining the data for all citizens for all calls) is considered unconstitutional.

"Law 298/2008 implements in the national legislation Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The legal regime of such a Community act foresees the obligation for the European Union member states related to the legal solution covered, but not to the concrete modalities on how the scope is being reached, the states enjoying a wide margin of solutions to adapt those regulations to the specificity of the legislation and national realities.

Neither the provisions of the Convention for defence of human rights and fundamental freedoms, nor the Romanian Constitution prohibit the legislative solutions of the state authorities interference in exerting the above mentioned rights, but the state intervention needs to respect strict rules, as explicitly specified in art 8 of the Convention, as well as in art 53 of the Romanian Constitution. Therefore, the legislative measure that affects the exerting of fundamental rights and freedoms must fulfil a legitimate purpose consisting of protecting national security, public safety, defence of public order, criminal prevention as well as protecting the rights and interests of other persons; to be necessary in a democratic society; to be proportionate with the situation that determined them; to be applied in a non-discriminatory way and to not affect the existence of such right or freedom.

- **What happened to data that had been retained before the ruling? Did the court sentence include an obligation to destroy these data?**

  No, the court sentence did not include such an obligation. According to the general regime of data protection, (law 677/2001 on data protection and ePrivacy law 506/2004), the data should have been deleted.

- **What happens to data retained that had been requested by any of the entitled bodies (police etc)? May these data be used by the said bodies/in a court proceeding?**

  Any provider that was requested to provide the data could, after the day of publication of the Constitutional ruling in the Official Monitor, refuse to hand over the data, as having no legal basis.

According to our information these data obtained based on data retention law could not be used in a court proceeding, as they could have been challenged as obtained by breaching constitutional rights.

10. Has new legislation been tabled or adopted after the Constitutional Court's ruling, in order to bring national law in line with the Directive?

As we've explained in answer no 2, officially there is no new legislation being drafted.

However, from an unofficial and un-quotable source, we found out a rumour that the Ministry of Communications and Information Society will try to suggest a new data retention law (the first draft was initiated by Ministry of Justice), however nothing was made public so far.

As explained on point no 2, there were no public discussions on this subject any more.

11. Please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Which cases are to be regarded as "emergency cases" so that access to the data may be sought by the Prosecutor without a court order for a maximum of 48 hours?

The entitled body needs to ask the Prosecutor to make a request to the President of the competent Court (or other Judge designated for this by him) to authorise the data request. The request needs to contain:

- "solid indications" that a serious crime is being prepared or perpetrated;
- the period of validity of the data request;
- name and centre of the legal person that has the data;
- the concerned person whose data is requested or indication the subscrbers' code or phone number;
- exact crimes for which he(she) is being investigated;
- the periode of time for the retain data requested.

This request can be made only when the penal proceeding has started.

The Court will examine if:

- it is the competent body to issue the request,
- the request had come from the competent Prosecutor,

- the penal proceeding has started,
- there are enough "solid indications" that a crime is being prepared or perpetrated,
- the crime is a serious crime according to the definition in the Romanian law,
- the other issues mentioned above that are included in the request,
- any other legal issues he deems appropriate to be ruled on.

As regards the "emergency cases" the text of the law is not clear, but they need to be clear indications that the retained data may be erased or lost or the crime would be committed right away if the Prosecutor does not act directly to ask the data.

The Judge that will need to approve this authorisation can also rules of this was an "emergency case" or not.

12. Please give more details about how EU legislative acts and international treaties on cross-border co-operation in data retention issues (including rules *specifically* designed for data retention as well as *general* rules applicable to data retention) are applied in Romania.

As far as we know there are no specific rules on data retention specifically.

There might be some rules applicable in this situation from the ratification of Romania of the Cybercrime Treaty and their implementation by law 161/2003 Title III[14].

However, the Romanian authority has only attributions, as foreseen in art 62, on quick freeze of data and seizures of devices that contain data, but not on the access to retained data.

Also, the Romanian authorities might send traffic data already in their possession, according to article 66 of the same law.

Art. 66 – The competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the crimes made by means of information systems or to solve the causes regarding these crimes.

13. Are the terms "non-commercial provider" and "provider for closed networks" (see your answer to question 24 of the first questionnaire) defined any further

[14] Unofficial English translation available here - http://www.legi-internet.ro/english/romanian-itc-legislation-and-articles/criminalitate-informatica/romanian-cybercrime-law.html

by law or jurisprudence? If not: what would be your understanding of how their meaning should be construed?

The terms "non-commercial provider" and "provider for closed networks" are not defined by law or jurisprudence. These are terms to define possible electronic communications providers (in the technical sense) that do not fit in the definition of the electronic communications legal framework and in the data retention law definition

Thus, the data retention law applies on:

a) providers of electronic communications network and services – the person which provides, for commercial purpose, services and/or electronic communication networks to the end users or other providers of electronic communications network and services, in order to sustain their traffic;

Consequently the law does not apply for persons that provide for non-commercial purposes these services. That would mean according to our understanding: NGOs, local associations that built their own network, educational institutions or even the Special Telecommunication Service (STS)[15] - that provides electronic communication services for some state institutions. (Presidency, Government, Ministry of Justice, Courts, etc.)

Also the law applies only to these electronic communication providers that have these services for:

- to the end users (retail)

– other providers of electronic communications network and services, in order to sustain their traffic (wholesale)

This excludes "provider for closed networks" which could be for example local flat owners associations that have a local network but provide these services only to the inhabitants of those flats.

14. **Could you please illustrate the "generic provisions that oblige any citizen to cooperate in good faith with the law enforcement authorities for crime prosecution": where in the law can this rule be found, and how far does it go (e.g. case law detailing the content of the rule)?**

This has been explained in answer no 3 in detail – it is more a principle than a specific text in the law.

15. **Please describe the generic rules of co-operation among the public authorities mentioned in your answer to question 33 (legal source where these rules can be**

[15] http://www.sts.ro/indexe.html

found and content thereof). Do these rules set any limits to the exchange of personal data?

The laws mentioned in Q33 only stipulate generic provisions such as Art 14 in the Law 14/1992[16] *(quoted below)* on the Romanian Intelligence Service, without providing any details. Usually the texts do not contain any reference to personal data. (according with art 2 para 7 of the data protection law, this does now apply to activities carried our for national defence or national security).

"In carrying out the powers incumbent upon it, the Romanian Intelligence Service shall collaborate with the External Intelligence Service, the Protection and Watch Service, the Ministry of National Defence, the Ministry of the Interior, the Ministry of Justice, the Public Ministry, the Ministry of Foreign Affairs, the Ministry of Economy and Finance, the General Direction of Customs as well as the other bodies of the public administration.

The bodies provided under paragraph 1 shall have the obligation to mutually grant the necessary support to one another in the carrying out of the powers provided by law."

16. **Please describe the content of the Order of the People's Ombudsman No. 52/2002 on minimal security obligations for processing personal data. Do the rules refer to national and/or European standards which are to be applied? If so: please describe their content.**

The Order 52[17] do not refer to any national and/or European standards, but some of its provisions seem to be inspired by some of them.

These obligations are set as guidelines for the data controllers to adopt and implement appropriate technical and organisational measures to ensure the confidentiality and integrity of personal data by their own safety procedures and policies.

The minimum safety requirements for personal data processing cover the following aspects:

l. User's identification and authentication

2. Access Type

3. Data Collection

4. Backups

---

[16] http://www.sri.ro/upload/law14.pdf

[17] Full text available in English on the Romanian DPA webpage - http://www.dataprotection.ro/servlet/ViewDocument?id=556

5. Computers and Access Devices

6. Access Files

7. Telecommunication Systems

8. Employees' Training

9. Computer Use

10. Data Printing

Update on the data retention report for Romania

Following a few years of relative silence on the matter, the Romanian government has initiated a new draft law on data retention in June 2011, following pressure from the European Commission that have announced the starting of an infringement procedure against Romania if the EU Data retention would not be implemented soon.

After a quick legislative procedure the new law was adopted by the Romanian Parliament and promulgated by the Romanian President, becoming this Law 82/2012[1] and published in the Official Monitor no. 406 from 18/06/2012. Adopted during a period of a national political turmoil, not enough number of MPs or the Ombudsman wanted to sent the law to the Constitutional Court for a pre-adoption procedure.

According to our information, no trial has been initiated until now from the civil society that could lead to a constitutional complaint.

The text of the new law is nothing else than a copycat of the former law 298/2008, that has been already declared unconstitutional. The only addition that is supposed to solve this problem is the new article 13 that says the data retention activity must fulfill the principles of same quality and security than other data used by electronic communication providers, and of "appropriate technical and organisational measures" for not losing or abusing the data (without making any reference to what that might mean in practice).

Instead, the present text is in fact vaguer than the initial law that was declared unconstitutional. The procedure to access the data has been deleted, just saying that the data might be accessed under the conditions of the "Penal procedure code and other special laws". Only that the current Penal procedure code does not foresee any procedure in this respect and, at least this moment, there are no special laws on the subject.

Also the right to access the data can now be exerted by any "judicial authorities" and "authorities with attributions for national security and safety", which was a vagueness of the text already criticized by the Constitutional Court.

The law adopted is actually worse than the initial one, with the access to the retained data in limbo. If the text of 2008 stated clearly that only a judge could allow the access to the data, the new text is unclear, making a reference to the Penal Procedure Code that, in fact, says nothing on the matter.

More information (all articles have been written by me)

New draft law for data retention in Romania (29.06.2011)
http://www.edri.org/edrigram/number9.13/new-draft-data-retention-romania

1 Text in Romanian available here http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-nr822012-privind-retinerea-datelor.html

Romanian Senate rejects the new data retention law (18.01.2012)
http://www.edri.org/edrigram/number10.1/romanian-senate-rejects-data-retention

Romanian Parliament adopts the data retention law. Again. (23.05.2012)
http://www.edri.org/edrigram/number10.10/romanian-parliament-adopts-data-retention-law-again