Chapter 18
Data Protection in the Clouds

Yves Poullet, Jean-Marc Van Gyseghem, Jean-Philippe Moiny, Jacques Gérard, and Claire Gayrel

18.1 Introduction

The Council of Europe (CoE) requested the Research Centre on IT and Law (CRID) to prepare a preliminary report identifying the main privacy issues related to cloud computing and the questions to be addressed in the future, in particular in the light of Council of Europe data protection standards and mainly of ETS 108 for the protection of individuals with regard to automatic processing of personal data (hereinafter referred to as ETS 108). This chapter is based on said report and as such, we chose to keep the report's structure, which is not the usual one for an article. In this perspective the conclusion is written under the form of questions which are open to discussion. This chapter does not aim to answer questions, but rather to raise them.

This chapter is structured as follows. It starts with a brief technical introduction illustrating the variety of services covered by the concept of "Cloud computing". As defined by the National Institute of Standards and Technology (NIST),[1]

> cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing services (hereinafter referred to as CCS's) include a large diversity of services going from those offered at the benefit of individuals – as the services

Y. Poullet (✉)
Research Centre on IT and Law (CRID), University of Namur, Namur, Belgium
e-mail: yves.poullet@fundp.ac.be

This chapter is based on the report written by the CRID in the context of the OCTOPUS Conference organised by the Council of Europe in order to strengthen the cooperation between Law Enforcement agencies under the Cybercrime Convention. The text of the report is available on the Council of Europe website. Even if the text of the article does represent a version deeply modified of the report, we have decided to limit the number of footnotes in order to keep the format of the report and to make reference not only but mainly to the text of the C.o.E Convention 108.

[1] Meil, P., and T. Grance. The NIST Definition of Cloud Computing, Version 15, 10-07-09, available on NIST (National Institute of Standards and Technology) web site.

S. Gutwirth et al. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, DOI 10.1007/978-94-007-0641-5_18,

offered by social networks – to those proposed at the benefit of companies in sharing a common software, or by using shared information infrastructures. Establishing a typology of cloud computing services is quite important because legal problems raised by each kind of computer services might be different to a certain extent. The second point is dedicated to the analysis of the adequacy of the ETS 108 definitions with the cloud computing reality. In particular, the status of the actors involved in the operations will be analysed. Thereinafter, our contribution analyses the duties of the persons subscribing to the cloud computing services or offering these services. Next, the crucial question of security is addressed. Finally, the chapter addresses the delicate questions of transborder data flows (hereinafter referred to as TBDF) and international private law, which are inherent to most of the cloud computing services.

Obviously cloud computing raises issues at many levels. Currently, cloud computing seems closer to fog than cloud and it might constitute a real danger for the users and data subjects whoever they are (legal entities, individuals).

Before analysing the different challenges raised by cloud computing services in views of the Data Protection legislations, let us try to explain why, with cloud computing, privacy issues have to be analysed in a deeply modified way. The first generation of data protection legislation took into account the sole risks linked to the processing by isolated information systems within a company or an administration. The risks of these systems were easily identifiable (sensitivity of data; processing purposes; etc). Nowadays, the terminals (PCs) are functioning in global and interactive networks with unprecedented options of exchanging more and more personal data. The network society has consequently raised new issues which are partly addressed by legislation like the EU 2002 e-privacy directive. The problems of confidentiality during the transmission, the need to regulate new types of data, such as traffic and location data, and the uptake of public communications services have significantly broadened the scope of the data protection. At the same time, terminals must be protected against illegal intrusion, and their functioning must be privacy compliant. With cloud computing, companies and administrations are invited to transmit their data, even their whole information assets, to the clouds by means of very user friendly web interfaces. The Cloud is, for obvious economic and security reasons, the answer to social pressure and provides individuals with the means to exist in the virtual society. The cloud computing service provider will use all the possibilities of the Net and of its information system, including those offered by other service providers for storing data, for ensuring their sharing amongst other users, and so on. What is quite noticeable is that, with cloud computing, the subscriber has lost the direct ownership/control of the information placed in the clouds because the data have left their own computer, or more generally their terminals, and are "somewhere in the cloud" in places determined by decisions, and notably the availability of the different elements of the Cloud Service operator's IT systems. These elements might be located in the same country as than subscriber's one, but often they are located somewhere else, even in non democratic countries. In other words, transborder data flows in the global network are becoming inherent to the essence of the CCS and the Internet is as such becoming the location of the processing of data. So starting from these premises, new challenges must be

addressed. In our view, cloud computing issues will constitute a major data protection challenge in the next future with questions such as: How to ensure a certain ownership/control of the data by the data subject? How to solve the delicate problem of TBDF?

18.1.1 Some Technical Aspects and Specific Risks Linked with Cloud Computing Services

18.1.1.1 A Brief History

Users make use of applications with many functionalities which help them in their work or in their other activities. They reasonably expect that their data be stored in protected spaces in order to retrieve these data when needed. That constitutes the standard way.

In the sixties, the computer users used mainframes for running software. The data were stored on tapes, with no direct access for users. Everything was "online". The users did not know where, and on which media, their data were stored. They only knew that the data were in one splendid and large room in one specific building. Everybody has seen these ranks of tape machines on TV. The data access was controlled by the operators of the mainframe. And no external access was possible.

Later on external access to computing services and data were created by means of modems and controlled (for the rare persons that could try to it) by passwords. With the advent of the personal computer, data storage and computing facilities became local, everyone could have programs and data on their own computer. Users became responsible for the access control to their data. Nowadays, with the Internet, users can access the data stored on many machines from everywhere in the world. With this comes responsibility of end-users for their own and other people's data.

Thus, simple users can access data on "mainframes" located anywhere. They can also access data they manage on their own system (that is to say their local network). Finally, they can access data stored in computers from where they have access when connecting themselves on Internet. Four main components are needed in each of these cases:

- Hardware (processing, storage and memory)
- Operating system
- Applications
- Data

The use of external information systems might bring certain advantages because it implies the possibility for outsourcing processing or support to larger facilities. Another benefit might be found in the fact that all the expenses and efforts concerning the maintenance, upgrades and security of the information system shared as part of the cloud computing service are financially supported by the different users of these services, and technically supported by the company offering the cloud

computing services. Cloud computing services in this sense do represent major scale economics for companies, particularly for small and medium-sized enterprises (SMEs). It should be underlined that this kind of benefit might be also offered in the context of a GRID. The main difference between GRID computing and the Cloud computing services mainly concerns the nature of the relationships between the users. GRID services concern users linked by a common professional interest and using the same information system (for instance, hospitals using the same datacenter or peculiar software in order to control their expenses). In the case of Cloud Computing services, services are not shared on equal footing by the users on the basis of individual agreements, but rather the selling of certain remote services, that we could describe as a commodity, by certain specialised (or not) companies. These commodities share the following characteristics:

- "On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service".[2]

This commodity can be offered through different deployment models. So, the NIST paper, already quoted, distinguishes:

[2]Meil, P., and T. Grance. The NIST Definition of Cloud Computing, Version 15, 10-07-09, available on NIST (National Institute of Standards and Technology) web site.

- "Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)".[3]

18.1.1.2 Cloud Computing

The model of cloud computing, at least for forms (SaaS), implies that there is a simple computer that runs a browser that accesses a remote service. Users can use the browser to interact with applications in the "cloud" and stock their data in a folder in the cloud. In this case, an important question is access to these resources (application and data).

Cloud services can be distinguished in three types: "software as a service", "platform as a service" and "infrastructure as a service":

- "Software as a service" (SaaS) is easy to understand: users access applications on the Web, for example, a word processor, a spreadsheet or email software. The services offered by Google (e.g., Google Docs, Gmail) are well known examples of SaaS. Data are also stored on the Cloud providers' IT systems. In such context, the CCS provider (e.g. Google) is technically responsible for the application services and for the data of the users (secure storage and secure access).
- "Platform as a service" (PaaS) offers an operating system where users can install their own applications. The platform provides services such as application services and database services. The data are stored depending on the application, either on the provider's system or locally on the client's system.[4]
- "Infrastructure as a service" (IaaS) offers one "logical hardware" infrastructure.[5] Users have to install their own operating system, the applications they need and they have to decide which Storage provider to use and they have to decide how

[3] Meil, P., and T. Grance. The NIST Definition of Cloud Computing, Version 15, 10-07-09, available on NIST (National Institute of Standards and Technology) web site.

[4] See https://www.dropbox.com/ for a simple example of a cloud storage facility or http://msdn.microsoft.com/en-us/azure/default.aspx for a more complex example of a platform provider.

[5] See for example http://aws.amazon.com/ec2/.

to connect the different PaaS components they use. In general the user can not determine where the data is physically located because the Storage provider will store several copies of the data at possibly changing locations.

At a high level, these three services are carried out through two kinds of elements in the cloud: datacenters and clusters. The datacenters are specialised hardware where data are stored. They generally provide security for access and recovery services. Clusters offer high performance computing facilities.

For simple cases, customers can use simple infrastructures. Virtual servers are examples of IaaS. The virtual computer installed by a user can be moved from one location to another when needed. The segmentation of the infrastructure must be serious, because, if not, one instance can read or write in one other instance or virtual machine.[6] Hacking or destruction is then possible.[7]

In the case of the SaaS, only data are separate. Each user starts one instance of an application (e.g. word processor). The identification of the user is the only way to attribute data to the correct user. For this reason, the system must have proper authentication methods in place. In the two other cases, the problem is more complex, but access control and security are important issues.

18.1.2 Specific Risks Associated with Cloud Computing

This section briefly describes some risks related to, or accentuated by, the use of CCS which would justify a possible intervention of the CoE. The rest of the chapter will go into some of them in greater depth. At this point we already have to make clear that the legal issues may vary depending on whether services are directed to individuals or to companies or even to public administrations. Each risk may require a specific assessment depending on the actors involved on both sides (demand and offer of CCSs).

As regards services offered to individuals, such as social network sites,[8] or other large public available web 2.0 platforms, the following risks can rise:

- The possibility – for a third party or the cloud computing service provider itself – to *profile data subjects* by linking several databases/information related to an individual represented in the CCS's databases or result of their use of the service. This risk increases when consumers are invited to use CCSs free of charge

[6] IaaS services are typically used by multiple tenants at the same time, and hence multiple virtual machines will run simultaneously on the physical server.

[7] Segmentation is also an important requirement for the other types of CSS because they share vulnerabilities.

[8] As regards these services, see Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking (WP163), adopted on 12 June 2009; Moiny, J.-P. "Facebook au regard des règles européennes concernant la protection des données", 2 E.C.J.L., 2010, pp. 235 and ff.

if they accept to receive one to one targeted adverts. They will be tempted to give privacy for "free" to CCSs.

- The concept of *consent*: when cloud users give up their privacy for services, their consent could not be free anymore. Beyond this risk, their consent can hardly be called sufficiently informed due to the opacity of many CCSs. Users are usually hardly aware of the true processing of their data, of cross-references made between different services, etc. Therefore, is consent still valid or aligned with the concepts of "free" and "explicit (informed consent)" which are its characteristics?
- For obvious reasons, *youngster's protection* might require additional measures. Is the consent by underage users valid? The US Children's Online Privacy Protection Act of 1998[9] requires parental consent for children aged under 13 years, and recently Article 29 Working Party has pleaded for forbidding the profiling of children[10].
- The problem of "*ownership*" of personal data: Consumers, once they have released their data in the cloud, might have difficulties not only to maintain access to these data (e.g., in cases of denial of access when they do not pay the service, or in case of bankruptcy of the CCS). But more fundamentally, they could have the difficulties exercise full control over the released data when they terminate their contractual relationship with the CCS. According to the general terms of many services, the provider could contractually reserve the right to keep the data even after such a termination (e.g., in the context of social network sites, where users commonly only have the option of deactivating their account instead of deleting it).
- Control over the data *after death*: when the subscriber of a service dies while his or her data are in a cloud computing system, who is then authorised to access these data (their heirs, the de cujus, the CCS)?

When a *company* subscribes to a CCS, additional questions might raise:

- The obvious need to distinguish clearly the concepts of user, subscriber and data subject, each of them referring to clearly different people involved into CCSs and being subject to different problems. So, the employee who is using the information system provided by his or her company might not be aware of the recourse made by his or her employer, the subscriber, to the cloud and to a CCS. As regards data located within the datacenters provided by the CCS provider, some are relating to customers, furnishers and so on, who are not necessarily aware of this fact. So to what extent can we consider that these persons are aware of the use of cloud computing services and is this recourse subject to possibilities of refusal or even of acceptance? Other specific questions relate to the distinction between

[9] See Sec. 1303, (b), 1, (a), ii of the Children's Online Privacy Protection Act of 1998, available on http://www.ftc.gov/ogc/coppa1.htm. Sec. 1303 (b), 2 however specifies some exceptions to the requirement of parental consent.

[10] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (WP171), adopted on 22 June 2010, p. 17.

users (employees) and subscribers (employers). In case of death of an employee, who will have access to data stored in the datacenter? If the user dies, may the CCS provider erase the identifier and password of this user? Is he authorised to do so? In the negative, who has the authority to do so? Beyond this question, is it conceivable, to the benefit of the employees using the companies' information system, to make a difference between private and professional, excluding the former from the use of cloud computing services?

- The *protection of legal persons* and their know-how, industrial secrets, etc. On this matter, two different problems are identified. First, the company might place trade secrets concerning itself or a third party on the cloud servers. Such trade secrets might be compromised by a lack of security of the CCS. Second, the cloud provider might record certain transactional data generated by the use of the offered services, which could reveal substantive activities of the company and, as the case may be, sensitive information about it. For instance, the storage and analysis of communication of financial data between the subscribing company and a bank might reveal risks of bankruptcy.
- The *exclusion or subjection of the use of CCSs to strict conditions when some types of data are processed or when particular activities are at stake* (like the activities submitted to a professional secrecy). Certain legislations (see for instance the US Health Insurance Portability and Accountability Act of 1996[11] on Health data) regulate the disclosure of data to third parties. Insofar as the cloud provider might be considered a third party, they will be submitted to such regulations. In some cases, it could be deemed, due to the sensitive nature of the data and the risks inherent to CCSs, that the processing of these data is not to occur in the cloud because of the dispersion of data and, to a certain extent, the loss of control by the data controller on the data stored within the clouds. This leads to the question of the ban of cloud computing as regards specific processing of personal data or activities. One can consider that some matters, such as health, justice or administration are so sensitive that they cannot be reconcilable with the use of cloud computing because of the potential spreading of information over the Internet and major risk of disclosure.
- For the same reasons, one may wonder whether CCSs should be forbidden or subject to certain restrictions when specific processing of data driven by public administrations or authorities are concerned. In some case, the use of CCSs could threaten the confidentiality of data and, as the case may be, jeopardize State's sovereignty, particularly as regards States' Security concerns. The use of hybrid clouds operating only within the national borders might be a solution to this particular problem.
- The *bankruptcy or transfer of the cloud computing activities* might cause certain problems. The cloud provider's bankruptcy might lead to the sale of the cloud

[11] Available on https://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf. About this example and others, see B. Gellman, Privacy in the clouds: Risks to Privacy and confidentiality from Cloud Computing, Report prepared for the World Privacy Forum, Feb. 23, 2009.

computing services to another company exercising competing activities with the subscriber's ones or having another privacy policy. The bankruptcy might in other cases lead to the termination of the activities. Anyway, the subscriber must be aware of the consequences of the disappearance or transfer of the cloud computing services on the data which are stored or put into circulation by it. So different questions would have to be analysed. Do we have to provide the continuity of the contract with its confidentiality or security guarantees, etc? Is it possible for the subscriber to unilaterally terminate the agreement for privacy or competition reasons and, if it is the case, to be sure to get back his or her data?

18.2 Personal Data Flows Within Any Cloud Computing System

Different personal data flows can be identified within any cloud computing system which involves several actors as the data controller, data processor, subscriber, user and data subject.

ETS 108 provides basic and useful definitions for the processing of personal data. However, this list does not take into account the peculiarities of cloud computing. Providing some additional definitions should clarify the understanding of the functions and duties of all the actors intervening in the cloud computing system. Any situation involving cloud computing can involve six major categories of actors – usually overlapping to some extent – and sometimes legally defined by ETS 108: a CCS provider, a subscriber to this service, data controllers, data processors, users and data subjects.

- *Cloud computing provider*: The natural or legal person providing a service (SaaS, PaaS and IaaS) in a Cloud computing system.
- *Subscriber*: The natural or legal person contracting with the cloud computing provider. It might be an individual (e.g., the average user of a social network site), a company or a public administration
- *User*: The natural or legal person actually using, in the context of his tasks, the CCSs. The user can be the same person as the subscriber, but also be a different person, such as an employee working in a company. This person would be the user, while the company would be the subscriber to the service (SaaS, PaaS and IaaS). In this respect, it could be assessed whether the cloud computing service provider should be subjected or not to specific obligations in favour of the user – only acting as a user? And which would be such obligations (e.g., a particular information duty)?
- *Data subject*: While ETS 108 already deals with the concept of "data subject", it doesn't give a complete definition. It appears important to precisely define this main actor in the personal data processing, whether in a Cloud computing system or not. To which extend, should we consider a legal body as a data subject to be protected on equal footing with individuals? Indeed, ETS 108 limits the concept

of data subject to individuals, thereby excluding legal bodies. Is such limitation still pertinent in a cloud computing environment?

- *Data processors and data controllers*: The distinction between data controller and data processor is at first glance quite clear according to the definition given by Directive 95/46/EC, but they are not defined by ETS 108[12]. The data controller processes data for his own purpose and defines the means to achieve this purpose; According to the article 2 (d) of the Directive 95/46, the data controller determines alone or jointly, both the purposes and the means of the processing of personal data, while the data processor operates data exclusively at the request of the data controller and does not pursue their own purpose[13].

In the context of cloud computing, the CCS provider might be considered in certain cases to be a data controller and in other cases as a data processor. It is quite clear, as recently asserted by the Article 29 working party,[14] that some CCS providers, for instance social networks, have to be qualified as data controller since they process personal data for their own purposes such as providing one to one marketing or transmitting data to third parties. The qualification might in other cases be quite difficult "since the cloud computing service provider could define in the broadest sense "means" of processing, that due to the characteristics of the service at stake, would justify some processing operations not directly requested by the subscriber – as the case may be, data controller". As an example, the provider of an IaaS, caring about the efficiency of its service, could automatically allocate processing and storage capacity between various facilities located worldwide. For instance, at a time "t", data centre and processing capabilities located in Germany are optimal. But, due to the increased use of these facilities at a time "t+1", it could be more sensible to have recourse to facilities located elsewhere in the world, for instance in India, in providing the service – which could involve a duplication of data, etc. In this respect, the technology at stake would automatically trigger a transborder data flow, the controller of which is not necessarily easy to determine. From another point of view, in a lot of cases, the cloud computing service provider might take advantage of storage or processing capacities offered by third parties, who could be considered as data processors of data processors.

In our opinion, it is difficult to qualify the CCS operator as data controller each time the processing operated by him are justified by the need to ensure the service proposed or to ameliorate it. It is quite obvious that the subscriber, by choosing a CCS operator, and by giving them certain latitude to define precisely how to achieve

[12] However, we can take the concept of data processor out of the article 7 of ETS 108.

[13] As regards the concepts of data controller and data processor of Directive 95/46/EC, see Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP169), adopted on 16 February 2010.

[14] WP169, Op. cit.

their tasks, determines the means of the processing. [15]The qualification of CCS as data controller or as data processor is a case by case decision. It depends from the possibility for the CCS to decide autonomously about the purposes of the data processing, knowing that the means might be trusted to a specialised service.

Even if we don't want to introduce "by force" the distinction between data controller and data processor in the context of a CoE amended Convention or by a specific recommendation, it would be necessary to specify the "legal" regime of this new actor and its specific duties. These duties concern, first, the subscriber having recourse to a data processor (obligation to have a written contract specifying the tasks given to the data processor, requirement as regards the quality of the data processor, etc) and, secondly, of the CCS operator independently of his qualification as data controller (prohibition or not of personal use of the data processed in the context of the tasks operated on behalf of the data controller, obligation to provide a high level of security, obligation to inform people in case of security breaches, etc.). It is quite clear that it would be wrong to assert that the only possibility to impose legal duties and obligations to CCS provider is linked to his qualification as data controller.

18.3 Domestic and Non Domestic Uses

Cloud computing serves the domestic and personal framework (e.g., social network sites, webmail, online blogs and word processors, etc), as well as professional environments (e.g., legal bodies decentralising their IT infrastructure to reduce costs, etc).

Bearing in mind that European Union has, voluntarily, limited the scope of Directive 95/46 to the non domestic processing of personal data, does this limitation remain relevant in the context of cloud computing? It is particularly relevant in the context of some cloud computing services such as social network sites. Here, individuals can make information concerning others available to the entire world, – rather than to a small circle of people who could qualify as household or domestic – which would make them a data controller.[16] A practical interpretation of domestic versus non domestic use has to be found which would not deprive data subjects of their rights enshrined in data protection legislation, and would not suffocate other individuals by heavy rules. As the case may be and depending on the cloud computing service at hand, it is necessary to think about the opportunity of establishing a softer data protection regime in spite of a wide application of an exemption to the scope of the legislation.

---

[15]In the same sense, we do not follow the Article 29 opinion referring to the SWIFT case, where the WP considers, a bit too rapidly and without appropriate nuances, that a furnisher of security services of data transmission become data controllers when they decide to answer to law enforcement agencies (LEA) requests. This would mean that a CCS providers would qualify as data controller each time they decide to answer positively to a lawful request issued by LEA.

[16]See the Lindqvist case which appeared before the European Court of Justice C 101/01 (2003).

This distinction might have harmful consequences for individuals as far as TBDF are concerned. Indeed and in some national laws, the rules dealing with such situations are applicable only to the non domestic use. This means that the data subject concerned by a non domestic process enjoys more protection than the others who could lack some protection in the context of cloud computing services.

18.4 The Protection of Legal Persons

Another issue resulting from cloud computing relates to the concept of personal data. Does this concept has to be confined to the definition given by the ETS 108 which says that personal data "means any information relating to an identified or identifiable individual ("data subject")[17]"?

In the context of, if need be, a specific regulation targeting cloud computing, wouldn't it be relevant to extend the concept of personal data to any information relating to an identified or identifiable *legal* person? In the surroundings of cloud computing, does the concept of personal data have to be extended – and how – to information such as industrial secrets, know-how, etc?

Most countries do not extend data protection scope to legal persons. The cloud computing system may change this conception because it will be used by the legal persons as a way to reduce their IT costs. And, depending on the relevant market, they could be deprived of any bargaining power (e.g., SMEs and non-profit organisations). This would compel them to contract under unfavourable conditions to stay competitive, having thereof less regards for data protection and privacy.

The extension of the scope of personal data from relating to persons to relating to legal persons is in line with decisions by the Strasbourg Court which has always asserted that article 8 ECHR protects not only the individuals but also legal persons notably their industrial secrets, know-how, etc.[18] Obviously, legal persons want to keep these safe from any disclosure to third parties without prior authorization. The concern is to determine to what extent a protection should be provided for by the law to legal persons, hearing that they can be economically and technically dependent on the use of CCSs. The information powers imbalance between individuals and companies or administrations created by IT use has been at the basis of data protection legislations.[19] Perhaps, it might be meaningful to extend data protection principles – at least some of them – to the protection of legal persons when it is clear that the same imbalance exists. And in so doing, the protection of the

[17] Article 2a.

[18] On that issue, see particularly, Bygrave, L. *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague/London/New York: Kluwer Law International, 2002, 448 pages.

[19] About the history of the privacy concept and the need to take fully into account the informational asymmetry between data subjects and data controllers, read notably Solove, D.J. "Conceptualizing Privacy", 90 California Law Review, 2002, 1085 et s.; Blok, P. Het recht op privacy, Boom Juridische uitgevers, 2003.

individual concerned by legal person's files or databases would also be improved. Furthermore it should be noticed that certain countries, members of the CoE, have already extended their data protection legislations to legal persons (see notably in Italy, Luxemburg, Norway and definitively in the E.U e-privacy Directive 2002/58 which was recently modified).

Therefore, these considerations coming from companies who may be major users of cloud computing systems, mainly on a B2B basis, have to be taken into account. Companies will store confidential information (such as the know-how, industrial secrets) on separate servers, or they will use cloud computing for internal communication (email, voice over IP, etc). Needless to say, they expect a reasonable protection of such information. And from an economic viewpoint, in case of lack of protection, they could be reluctant to use cloud computing systems.

A better protection of data related to legal persons may be necessary due to the economic pressures that could lead companies to adopt the cloud computing paradigm. Indeed, "meta-processing" is possible within such cloud systems because their providers may access information of various legal persons. With such a cross-source of data, CCSs providers could offer added value services (e.g. risk analysis on companies) to third parties. Such behaviour may constitute a major risk of disclosure of confidential or sensitive information to third parties.

Taking these concerns into account, it has to be determined if the concepts of personal data and data subject have to be extended to legal persons as regards cloud computing. Arguments might be drawn down from previous extension to legal persons as it has been the case as previously underlined under the EU e-Privacy Directive and under certain legislations of member states of the Council of Europe (Italy, Norway, Luxemburg, etc).

18.5 Liability of the Actors

Primary issues relate to the concepts of data controller and data processor. As has been argued earlier, the cloud computing system will involve both of them. The main question is to define who is who and who does what. For sure, the data controller *is the cornerstone of the data protection regulation*. The data controller has the responsibility of the main duties (information, security, etc). The determination of the data controller will have a huge impact on the legal structure of the cloud computing system.

In the identification of the data controllers involved in the cloud, we have to take into account the extraterritorial characteristic of actors and its consequences. Indeed, numerous CCS providers are set up out of the territories under the jurisdiction of the CoE's member States. Consequently, the control of the behaviour of the CCS provider can be difficult for both the authorities and the subscribers, as well as for the data subjects. Which then leads to difficulties as regards the control of the respect of the duties enshrined in data protection legislations, and as regards the sentence of the breach of these legislations.

As suggested, in some cases the CCS provider can be viewed as a data processor instead of as a data controller. According to this view, they can only act on behalf of the user (or subscriber) who himself processes personal data. But sometimes, the CCS operator pursues its own purposes for the processing of personal data. And as far as this processing is concerned, it is a data controller. Two issues result from this assessment. First, when a Cloud Computing service provider is data controller and data processor as regards a same user (or subscriber) could it be deemed appropriate and/or necessary to extend its quality of data controller for the whole processing operations? Secondly, if it is only a data processor, is it appropriate and/or necessary to establish, as the case may be, some specific duties (e.g., security, information, etc) and/or a specific rule of responsibility?

Of course, it appears preferable that data controllers be under CoE's member states' jurisdiction. The question directly relates to the right of protection of the users and data subjects. Then if the main actor is outside the scope of Europe's jurisdiction, how can the data subject or the subscriber or even the authorities control the processing of personal data and sue CCS providers if they breach their duties?

Consequently, from the data protection point of view, the following question raises: when is a CCS provider a data controller – or even a "joint-controller" – or a data processor?

A third option would be having the subscriber/user and the CCS considered jointly as data controller.

BUT the question raised by those three scenarios is whether it is possible for subscribers to require by contract with the CCS operator that the data generated or operated through their cloud computing services are located in the territories of the Member states and to forbid any onward transfer? What about the possibility for users to take benefit of this provision? A third party beneficiary provision ought to be included in cloud computing standard contract. At this point, we only lay down the question which will be elaborated in Section 18.9 when we will deal with the TBDF issues

However, it has to be pointed out that in practice, both models could, in some extent and in a same relationship between the CCS provider and its subscriber, overlap. Depending on the processing at stake, the provider could be data controller and data processor at the same time with regard to the same data or to the same data subjects. In this respect, it has to be determined if the subscriber – following a basic view, that is to say the data controller – could be a co-controller as regards the processing the controller of which is the provider – following the same basic view, that is to say the data processor. To this end, the following fundamental question can be raised: how to define "joint-controllers" and does such a definition have to be adapted in the context of the cloud computing? This is of course crucial due to the aforementioned scattered location of the actors of the cloud.

The following simple examples can illustrate the pertinence of the purpose. An employer decides to have recourse to encoding software offered by the cloud (SaaS) and designed to encode invoices from employees who seek refund for fees supported by them. The SaaS provider could offer its subscriber (employer) an additional – of course paid for – service to monitor the expenses of his employees. The service

could consist of the sending of monthly reports detailing in descending order the total amounts of expenses per employee. In such a case, could – and should – the purpose of the processing – monitoring of employees in a specific field – being a complementary service, be deemed to be defined by the subscriber and the provider at once?

Another example comes from the social network sites context. The provider of such a network could offer a personalised advertisement service consisting of a SaaS enabling a company to choose a specific audience to deliver advertisements, without such company processing any personal data, the provider of the SaaS holding alone this task.[20] Could – and should – the company ordering the advertising campaign be deemed to be a co-controller of the processing at stake? In both cases, the providers of SaaS define means for the processing of personal data and suggest to subscribers a purpose they assigned to the means they created, purpose the subscriber chooses to appropriate, bearing processing of personal data. The very question is then the following: is it opportune to define – or redefine – a "joint-responsibility" of the actors in such cases, and how could and should it be done?

If the ETS 108 imposes duties on the data controller (controller of the file), there is nothing concerning the data processor since this latter is not considered by ETS 108[21] (even if we find this concept in embryonic form in the article 7 of ETS 108). Being a main actor of the cloud, it might be useful – and this has to be assessed – to impose on data processors themselves – or, as the case may be, on some data processors – specific duties by "law" instead of contract. Clearly, where a data controller does not have the bargaining power to impose their own warranties as regards data protection, the law could mitigate such an imbalance of powers. The specific duties of the data processors CCS providers could consist of security obligations, information obligations, a specific liability (e.g., as what exists as regards the responsibility of the intermediaries at the sense of the e-commerce Directive 2000/31/EC). As stated above, a particular liability could be established as regards joint-controllers. But this has to be further assessed. And the present considerations are of high importance since each time it is considered opportune to create new duties, the question of liability has of course to be studied.

18.6 Transparency and Duties of Information Including in Case of Security Breaches

We have to make distinction between the three situation drafted above. Depending on the role of each party, the duty of transparency/information towards the users and data subjects will be different. Nevertheless, this duty should be a fundamental objective of any cloud computing system. This objective involves the *information*

[20] See for example J.-P. Moiny, Op. cit., pp. 249–250.

[21] However, we can take the concept of data processor out of the article 7.

obligations definitively with regards to the users, but also perhaps more generally with regards to all the data subjects.

Providers are compelled by information duties if they are data controller. However, if the CCS provider is also a data controller pursuing his own purpose as regards data related to the users of the service, the subscriber has no duty, according to data protection rules, to inform the users of such a processing if he is not involved in the processing as data subject.

Moreover, if the CCS provider is only a data processor, the subscriber only outsourcing his IT infrastructure, in our view, users should be informed of the recourse to cloud computing technologies by the data controller. Finally, it needs also to be asked if a data controller relying on a CCS provider as data processor should not inform the data subject of this practice. Indeed, the use or not of a CCS could be decisive as regards the data subject's consent. This data subject does not necessarily want to send personal data to an unknown third party who is not his direct contractor, especially if he has no certainty about the final place of the processing.

Next to the general information duty enshrined in article 8 of ETS 108, article 5a of ETS 108 also concerns the transparency of the processing of personal data. It sets that the "*personal data undergoing automatic processing shall be obtained and processed fairly and lawfully*". The term "fairly" involves this concept of information. And it could be argued that it is unfair to rely on CCSs without informing users, as the case may be, even in the situation where the subscriber and the CCS provider are not data controllers. Therefore, it might be suggested to modify article 5a of Convention 108 in order to fit the specific transparency issues raised in any cloud computing system. In this respect, it needs to be determined to what extent the data subject has to be informed of the particular technology at stake and its technical implications, such as the relocation of the storage of information in another State, the chain of sub-processors, and, as the case may be, its legal implications such as the occurring of processing operations in a non Contracting States where even adequate – but different – data protection rules merits mention?

Still as regards the evolution of the ETS 108, or even in the framework of a CoE recommendation, it would be of high interest to consider the introduction of a *duty of information related to security breaches*.

Indeed, the concept of security breach is unknown by the CoE regulatory text, but has been introduced recently in European Union by the Amending Directive on e-privacy. This Directive defines "personal data breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. The main idea is to put on the shoulders of certain communication services providers' new obligations provided that specific risks are linked with the nature of their services.

As regards, European Union Directive, the targeted services are limited to publicly available electronic communication services even if it has been recognised that in the future the concept must be extended to other services due to the risks existing in other services like banking on line services or electronic healthcare online

services. Clearly the debate around the revision has asserted the need to re-open the debate about this limited scope and to follow the US example (see at the Federal level, the "Data Accountability and Trust Act", by extending certain obligations to any person engaged in interstate trade and who own or possesses electronic personal data shall notify a breach to individuals, if the breach leads to an unauthorised third person acquiring the data, and also to the Federal Trade Commission. So the first question is: "To what extent the specific nature of the risks linked with cloud computing services might justify the extension to these services?" Perhaps the U.S. extension or the extension to all cloud computing services is too broad since they will conduct to minimise the obligations to impose but considering the nature of the risks offered by cloud computing services acting or not as data controller and offering not a specific services like a service assisting people in order to fix meetings (like Doodle) but services including more sensitive processing, what remains to be defined. The main criterion must be the importance of risks incurred by the subscriber of the service but more generally by the concerned people.

The second question, having solved positively the first one, envisages the different obligations linked with the "Security Breach" regime. It consists of two kinds of additional obligations:

- First, all the legislation imposes a duty to inform the data subject through appropriate means, which might in case of cloud computing services go far beyond both the subscriber or the users and implies in cases of cloud computing offering purely technical or software facilities without having access to the data themselves a partition of the tasks between the service provider and the subscriber and that in order to afford them an opportunity to take the needed measures to avoiding or reducing the risk. As regards the list of the beneficiaries of this obligation, can we consider, on the basis of the previous remarks, that in certain cases this obligation to notify must be extended at the benefit not only of individuals but also of legal persons?
- Second point, does the legislator have to impose an obligation to alert at the same time the data protection authority? But in case of positive answer: which one (due to the global character of the provider)? Which information must be given? And through which channel?

Finally one pinpoints the idea for standardisation authorities of establishing in close connection with these independent agencies technical and security means.

18.7 Security

18.7.1 Introduction

The cloud computing pattern implies two main categories of data flows. A first one relates to the flows between users/subscribers and the cloud infrastructure. And a

second one which groups the data transfers within the cloud system together. In such a context, two levels of security therefore have to be distinguished. The first one deals with the connection between the user and the cloud computing provider. And the second one relates to the cloud computing system itself.

Through this distinction, the cloud computing system is considered and promoted by their providers as a kind of safety deposit box which can be accessible only by authorised person. This is possible for SaaS services where the CCS provider assures that no other cloud services are used to provide the SaaS service or an IaaS, PaaS service where only one instance is used. In a PaaS, IaaS context complex systems can be realised. The single components and additional storage services are connected over the internet. The same is true for an SaaS service using other cloud services.

On the other side, the access to this safety deposit box must be secured to avoid any access to the transferred data by unauthorised persons. Such access should usually occur through the Internet as it should also most probably be the case of numerous data flows within the cloud. This clearly shows that Internet access providers (IAPs) also have a fundamental role in the cloud infrastructure as regards the conveyance of signals between users and the cloud system, but also within the cloud itself. IAPs offer an IP connection. Based on this connection secure environments such as VPNs can be realised between the endpoints of the communication, hence the system of the user and the system of the cloud provider.

Article 7 of ETS 108 imposes "*appropriate security measures*". It does not define who has to fulfil this obligation. It might be the data controller, the data processor or even the sub processor (even though these two last actors are not defined by the ETS 108 even though we could consider that the first one exists in an embryonic form). The concept of "security" is quite broad, even if not defined precisely by the article 7 of ETS 108. It means under article 17(1) of the Data Protection Directive, protection "*against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing*". So, for example, the risk of wiretapping by unauthorized third parties during the use of the services requires appropriate safeguards like the use of cryptography or secured lines (e.g., in case of electronic transmission of the credit card number). The possibility of intrusion within the provider's information system in order to collect all its customers' addresses or to manipulate certain data, imposes the necessity to install firewalls and other security measures. The sending of worms through the information systems of a communications service provider or the creation of a mirror site in order to lead astray certain communication are other specific risks linked with the use of communications services. The obligation is not limited to technical measures but encompasses also organizational measures which might be the nomination of a data security manager competent to ensure the compliance of the functioning of the service with all Data protection requirements.

Security is essential in case of CCSs since it is quite clear that by trusting a cloud computing service, the subscriber aims at being protected against all risks linked not only with confidentiality (disclosure or intrusion), but also with integrity

and availability of the data stored somewhere in the cloud. In other words, because the cloud computing service provider is offering services founded on security in the broadest sense, it seems meaningful to impose them additional obligations as regards this obligation to security and more particularly in case of what is called: "security breach".

18.7.2 Specific Security Obligations

Regarding security and integrity of CCSs, according to the peculiar risks raised by such services due to the concentration of applications and or data used by different users and subscribers and the huge possibility for unauthorised people of aggregating all these data, it might be wise to impose new obligations on their providers. Amongst these appropriate security measures, three ones could be taken into consideration: The first one addresses the problem of unauthorised access by the provider's employees: providers of cloud computing services could be subject to an obligation to develop measures like identity management systems in order to fix and effectively control the respective privilege afforded to each member of personnel regarding access to personal data conveyed, stored or operated by the communications services. The second one would target the necessary protection of these data against any loss, destruction or illegal access or storage. This refers to various technological security measures such as the encryption of transmitted data, the adoption of automated control systems about the quality and integrity of stored or transmitted data, the setting up of log-in and log-out registries, etc. The last security measures would concern the adoption by the provider to express in clear language their security policy. This obligation contributes to an increasing accountability of the data controllers by compelling them to envisage the risks associated with the services they provide, to define exactly how they manage these risks and by making them responsible in case of non respect of their commitments. Furthermore it might be envisaged that the cloud computing services' provider would be required to cooperate with the competent data protection authority(ies) in case they would like to audit the security measures promised or implemented by the providers. In the same line, the possibility for these authorities or standardisation authorities to issue recommendations on best security practices ought to be assessed.

Some other organisational measures may be adopted in the context of the cloud computing matter as:

- Obligation to audit the system to put the risks and the lack of securities or confidentiality in an obvious place;
- Obligation to segregate the data stored by each subscriber in cases of multitenancy in order to avoid any accidental or unlawful access to these data by another subscriber;
- Obligation to have a person responsible for the security who will be in charge to warrant the security of the cloud computing system for the provider;

- Standardisation/normalisation of the sector to give to the user/subscriber a kind of security in its choice. This standardisation/normalisation goes hand in hand with the delivery of quality-labels available for cloud computing providers who insure the respect of several conditions/obligations of quality.

The Cloud Computing business model and architecture calls for a deeper examination of the relevance of non regulatory instruments. Indeed, cloud computing companies are mostly international and implemented in a great number of countries. Advantages and disadvantages of self-regulatory instruments, such as the European Union model of Binding Corporate Rules (BCR), whether as an alternative or complement to the existing legal framework, need to be assessed. Due to the globalised nature of cloud computing companies, we strongly believe that the European Union's experience with BCR could provide an interesting framework and point of departure for future debates.

18.8 Transborder Data Flows and Applicable Law to the Processing of Personal Data

Due to its highly virtualised architecture, CCSs involve great amount of data transfers, among which personal data as defined in the ETS 108, and by thus raise the issue of the applicability of the transborder data flows (TBDF) regime defined in the Additional Protocol 181. First, these transfers may occur between several actors: personal data may be transferred within the cloud provider's proprietary cloud, which can cover several countries; transfers may occur between cloud providers; transfers also occur between the cloud subscriber and his cloud provider, when he benefits from the cloud computing services wherever his location, such as when accessing, consulting or downloading personal data. Second, these transfers between actors may pursue different purposes: some transfers might be justified for purposes of transit or technical maintenance, while others are directly justified by the necessity to provide the CCSs requested by the user.

All these transfers may involve TBDF, since the cloud providers may resort to processing materials located in several countries to offer its services to subscribers/users soliciting cloud services from anyplace. Circulation of information, and as far as we are concerned, of personal data within and outside the cloud may occur in non State Parties to the ETS 108, among which most do not provide adequate level of protection. This state of fact raises the following issue.

18.8.1 Applicability of the Existing Legal Framework of Additional Protocol 181

The applicability of the existing legal framework to cloud computing technology requires deeper attention and assessment. Article 2 of additional protocol 181

basically prohibits international transfers of personal data toward states not party to the ETS 108 that would not ensure *adequate level of protection*. Any actor involved in cloud computing services, whether user, subscriber or cloud provider, should be fully aware of this prohibition and the legal risks associated with international transfers that would not satisfy the TBDF regime. It is obvious that in the context of contractual relationships between CCS providers and their subscribers, the last ones might impose certain restrictions to the first ones imposing for instance that the storage of data and their processing have to be operated in the country of the subscriber (certain governments impose that kind of restriction) or in specific countries where the adequate protection is obvious. This kind of "Zoning the Net"[22] could also be imposed through the design of the networks' infrastructure like SWIFT would have decided, according to its public statement, since January 2010. According to that decision, transfers concerning European citizens would be operated exclusively through the SWIFT European network. It would be possible to have, for certain types of data like sensitive ones, legislative mandatory rules prohibiting the use by CCS of their global networks in order to avoid risks of onward transfers to countries where no adequate protection is offered.

Derogations to this general prohibition as provided in additional protocol 181 need further examination. As provided in article 2 a), national laws may allow transfers of personal data toward non-adequate destinations in case of "*specific interests of the data subject*" or when legitimate interests, especially important public interests prevail. Rightly applied, these exemptions could constitute a basis for several international transfers in the cloud computing context. As a first instance, the data subject's consent to the transfers at stake could be solicited. As a second instance, international transfers could be justified by the necessity of the performance of the contract concluded in the interest of the data subject between the cloud provider and the cloud subscriber/controller. Public authorities resorting to cloud computing services in the framework of their tasks could justify international transfers in the name of legitimate important interests.

As far as the second set of exemptions is concerned, article 2, b) offers possibilities of international transfers "if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law". Appropriate contractual clauses might constitute a relevant framework to ensure the legality of international transfers. However, such framework needs further assessment about its relevance in the cloud computing context, due to the necessity to take fully into account that the flows generated by the CCS'es often are concerning a lot of countries and a lot of companies as previously asserted. Perhaps the use of "Binding Corporate rules" adopted by large multinational companies offering cloud computing services can be at least a partial solution.

---

[22] The idea to come back notwithstanding the global character of the Internet to a certain "zoning" of the Net in order to ensure the sovereignty of the countries and national values, has been developed by Joel Reidenberg (Reidenberg, J. "Technology and Internet Jurisdiction", 153 UNIV. OF PENN. L. REV. 1951 (2005)).

In general, the applicability of these two sets of derogations to the cloud computing context needs further assessment from the point of view of the level of data protection aimed at by the CoE. In the context of unbalanced relationship between a cloud provider and its subscribers that could either be individuals or legal persons of little/medium influence, raising the data subject's consent or the necessity to perform a contract concluded between the cloud provider and the customer as primaries legitimate legal basis for international transfers could reveal wholly unsatisfactory. As regards the legitimacy of the TBDF based on the necessity of the performance of the contract, it might be questionable to ground flows as regards users or more generally data subjects having no contractual relationships with the CCS operators by the necessity of the performance of the contract concluded between the CCS and the subscriber author of these TBDF.

18.8.2 International Transfers of Personal Data/Storage of Personal Data and Law Enforcement Objectives

One of the most obvious and serious risks for data protection raised in the context of cloud computing architecture is a massive access by law enforcement authorities to the personal data and information stored in datacenters. Indeed, these datacenters can be established in countries that provide little or no protection of personal data in the framework of law enforcement activities. The development of datacenters might provide great opportunities to public authorities to access to great amount of information pertaining to its citizens or to foreign citizens.[23] Even considering democratic countries, the United States of America constitute a problematic example due to the very controversy third party data issue in the limited scope of the Fourth Amendment protection. We will come back on that issue.

18.8.3 Limitations to Transborder Flows and Applicable Law to the Processing of Personal Data

Cloud computing technologies involve countless TBDF. As regards the viewpoint of the CoE, these flows implicate Parties to the ETS 108 and its additional protocol (including European Union member States), as much as foreign States. A first set of rules is provided for in article 12 of the ETS 108 in consideration of TBDF *between*

[23] Except in cases where onion routing is used by cloud computing service. Onion routing is a technique allowing anonymous transactions within a computer network. The messages are encrypted repeatedly and sent through multiple networks nodes called onion routers. Each node decrypts the message in order to get the routing instruction and so encrypts and sends the message to the next onion router till the final destination. Intermediary nodes do not know the origin and the final destination of the message. In that case the national law enforcement agencies are unable to get access to the information if it is transmitted through onion router to a destination outside the national borders. On onion router example, see EFF'sTor: http://www.torproject.org.

Parties to this Convention – only indirectly taking into account TBDF intended for non contracting States (article 12.3, b). And a second one, provided for in article 2 of the additional protocol, directly addresses the issue of TBDF intended towards *non contracting States*. It has also to be underlined that the member States of the European Union have also to apply the TBDF regime provided for by Directive 95/46/EC (in particular, articles 25 and 26).

The aforementioned rules of ETS 108 pursue the specific aim of reconciling guarantying effective data protection and fundamental rights and liberties – even outside national borders – on the one hand, and on the other hand, ensuring the free international circulation of information between people, as the case may be, avoiding forms of protectionism. In this respect, TBDF *between Contracting States* should not be subject to any *special controls*; "in principle there shall not be permitted between Contracting States obstacles to transborder data follows in the form of *prohibitions* or *special authorisations* of data transfers"[24] (emphasis added by authors). Therefore, the ETS 108 prohibits what could be called an "administrative control" of data flows.

However, according to (article 12.3, a), a Party can disregard this rule if it has specific legislation for certain categories of personal data or for *automated personal data files*, because of the nature of those data or those files, except where the legislation of the other Party provide an equivalent protection. So, it can be asked whether CCS could – and should be, for instance due to the characteristics of the service at stake – deemed to constitute such a category of «automated personal *data file*» (e.g., health care online services) that needs to receive a specific treatment? In other words, in the context of CCS and its particular risks, the obligation imposed by the ETS 108 to the contracting States to adopt a particular regulation (e.g., concerning the processing of sensitive data through CCS) has to be assessed. As stated above, cloud computing covers various scenarios and it could require specific rules and particular treatment in some cases and not in others (e.g., depending on the public nature of the CCS, on the nature of the beneficiary of the service who can be a consumer, a children, a private corporation or a public administration).

As far as the additional protocol and the TBDF implying *non contracting States* are concerned, and except the exceptions provided for in article 2.2 of the additional protocol, article 2.1 of the latter compels contracting States to forbid these flows if the concerned non contracting State (or organisation) does not ensure an *adequate* level of protection for the intended data transfers. In this respect, the assessment of adequacy could be realised on a case by case basis. And it can relate to the processing of personal data for criminal investigation purposes by State agencies, or even for any "public" purpose (criminality, taxation, immigration, etc). In this respect, as the Directive 95/46/EC also forbids European States to authorise TBDF towards foreign States not ensuring an adequate protection, the adequacy assessment does not take into consideration the "processing operations concerning public security, defense, State security (including the economic well-being of the State when the

[24] Explanatory Report of the ETS 108, § 67.

processing operation relates to State security matters) and the activities of the State in areas of criminal law".[25] Therefore, to some extent, ETS 108 offers some added value. Anyway, due to the diversity of CCS, some distinctions could be drawn by the contracting States to ETS 108, and the protection offered by one foreign State could be adequate in one case and not in another. Which distinctions can and should/have to be drawn in this respect?

Two principal remarks can be made as regards TBDF directed towards non contracting States.

Firstly, the aforementioned rule should be without prejudice to an analogical – and *a fortiori* – interpretation of (article 12.3, a) of the ETS 108 in the present context of TBDF targeted to non contracting States. That is to say that the Convention should be interpreted in such a way that a contracting State can prohibit – or subject to authorisation – a TBDF related to a specific "automated personal data files" aforementioned if, for instance, the foreign State concerned does not offer an equivalent protection, *even though* it ensures an adequate level of protection. Restrictions to TBDF allowed between contracting States are *a fortiori* allowed between contracting and non contracting States.

Secondly and more generally, the additional protocol doesn't compel the contracting States to do anything else if the targeted foreign State offers an adequate level of protection; it only forbids allowing TBDF targeted to non contracting States. In this respect, despite the fact that the protocol also pursues the free flow of information, it does not explicitly prevent contracting State to forbid personal data flows targeted to a non contracting State offering an adequate protection. The same conclusions also apply as regards Directive 95/46/EC. So, the question in the context of cloud computing and TBDF to foreign States is also the following: could a contracting State deem that a particular processing involved in a CCS require an equivalent protection from the non contracting State, even if this particular processing is not deemed to constitute a particular "automated personal data files" under article 12.3, b) of the ETS 108, or to involve particular data? In other words, contracting States seems here to recover a larger margin of discretion than was the case under the ETS 108. But, on the one hand, how significant is this discretion? And, on the other hand, which CCS could and should/has to be specially treated through this potential margin?

Beyond what has been called an "administrative control" of TBDF, ETS 108 and its additional protocol, although they try to solve – in a certain manner – the issue of TBDF, do not provide for any rule related to the question of the applicable law to the processing of personal data. And this is also true regarding personal data flows between contracting States. As far as these latter are concerned, the explanatory report recognises that "it may not always be easy to determine which [. . .] national law applies", and it underlines that "the "common core" will result in a harmonization of the laws of the Contracting States and hence decrease the possibility of conflicts of law or jurisdiction". However, neither the Convention, nor the

[25] Article 3.2 of Directive 95/46/EC. These matters are outside the scope of Directive 95/46.

additional Protocol addresses the issue of applicable law. Moreover, the Explanatory Report also specifies that the principle of freedom of flow of personal data provided for in article 12.2 "does not mean that a Contracting State may not take certain measures to keep itself informed of data traffic between its territory and that of another Contracting State, for example by means of declarations to be submitted by controllers of data files". In the context of cloud computing, the scattered worldwide locations of the involved actors (i.e. CCS providers, subscribers, users and data subjects, controllers or processors) exacerbate conflict of laws concerns – that already existed – and have to be faced by national legislations; but how can they regulate and which constraints limit their margin? It is clear that harmonisation of the data protection rules is useful and that people (users and providers of the cloud) will benefit from such harmonisation. However, where no complete harmonisation exists in an inherently international context, a – common – conflict of law rule could bring some legal certainty.

European data protection law addresses, to some extent, the question of the applicable law through *Directive 95/46/EC*. This latter compels Member States to apply their national laws in the cases defined in article 4 of the directive.[26] This article marks the spatial boundaries of European data protection law. It seems that this rule needs to be implemented as a "unilateral conflict of law rule" defining the applicability of the national law at stake following the defined criterions. However, despite the fact that the directive also provides rules as regards TBDF targeted to a non Member State, it does not provide for a general "bilateral conflict of laws rule", that is to say a rule determining which law (of any State) apply to which situations. Therefore, the Member States could be deemed free to adopt their own conflict of law rules as far as they comply with article 4 of Directive 95/46/EC.

Contracting States (here, the legislator or the jurisdictions) have to define which law applies to which particular processing of personal data. And they have different ways to determine the applicable law. They can adopt a bilateral conflict of laws rule determining the applicable law in all instance (bilateral method), they can define the criteria of applicability of their law (for instance, taking into account the place of establishment of the data controller and/or the location of the equipments it uses for the purposes of a particular processing, see art. 4 of the directive 95/46/EC) with an unilateral rule (unilateral method), or they can also define a particular "public order

[26] As regards this rule, see notably Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56, adopted on 30 May 2002; Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines (WP148), adopted on 4 April 2008, pp. 9–12; Article 29 Data Protection Working Party, Working document on Privacy on the Internet – An integrated EU Approach to On-line Data Protection – (WP37), adopted on 21st November 2000, p. 28; J.-P. Moiny, Op. cit., pp. 255–270. As regards data protection and jurisdiction, see in general C. Kuner, "Data Protection Law and International Jurisdiction on the Internet", Parts 1 and 2, 18 (2 and 3). *International Journal of Law and Information Technology*, 2010: 176–193, the second part will be published in a forthcoming number of the same review.

exception clause" compelling judges to apply national law in some specific cases or when the application of a foreign law leads to unwanted results.

In any case, cloud computing technologies require a reflection on part of contracting States to the Convention of the CoE on which criteria are the best ones to determine the applicability of their national data protection laws and to accommodate the particular issues arising from the above mentioned technologies. In this respect, for example, only some data protection rules could receive a particular territorial scope as regards cloud computing services in general or even some cloud computing services in particular. For instance, specific duties regarding information and right of access could have a more extended territorial scope if some data protection rules are extended to the processors, imposing them specific duties or responsibilities – if deemed necessary in the evolution of data protection law. And the applicability of these rules could depend on specific criteria differing from those applicable to the data controller according to already established general data protection rules. Needless to say, such a conflict of laws rule would gain in quality – from a practical point of view – if it would be discussed at an international level – for instance, under the auspices of the CoE. It should also be noted that directive 95/46/EC is under review. A discussion relating to conflicts of law seems to be of high interest and pressing to guarantee the practical enforcement of data subjects' protection, and to bring legal certainty to the emergent and promising market of cloud computing.

In such a reflection, it is required to take the technical peculiarities of CCS into consideration, for instance to avoid using irrelevant links with the territories of the State whose law has to apply. For instance, the place of the equipments used for the processing of personal data can be solely the result of efficiency considerations related to the working of the cloud. In this case, such a location seems less relevant as regards the identification of the applicable law, while Directive 95/46/EC links the determination of the applicable law to the location of the equipments used for the processing at stake. However, it has to be noted that the location of the processing capabilities can also help bringing legal certainty by localising the CCS offered in a specific geographic area to ensure the applicability of a specific legislation. It could be a convenient way to avoid conflict of law and to provide a wide range of services taking into account users wishes as regards data protection rules. The place of establishment of the CCS provider can also be of little relevance when this provider purposefully offers its services to consumers located in another country than the country where he is established.

A final point can be underlined as regards the applicable law to the processing of personal data and the TBDF's involved in the context of CCS: which influence would article 8 of the European Convention on Human Rights (ECHR) have on the international processing of personal data and on conflict of law?

Article 1 ECHR reads as follows: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention". In this respect, the jurisdictions of these contracting Parties, applying the law of a non-contracting State of the ECHR, could have to ignore this foreign law if, in the particular case, it rises to a conflicting situation with the fundamental

rights provided for by the ECHR.[27] For instance, the European Court of Human Rights has already approached the concern of the influence of the ECHR on private international law as regards article 6 ECHR and the exequatur of a foreign judgment.[28] Four questions need to be addressed. Firstly, which "rights" recognised under article 8 ECHR could influence the application, in a particular case, of conflict of laws rules? Secondly, which data protection rules fall within the scope of article 8 ECHR and these rights? For instance, which rules of the "common core" of the [ETS] 108"? It should be kept in mind to this respect that data protection rules proceed to the "horizontalization" of the human right to privacy in the information society. And finally, which "connections" an international case involving cloud computing technologies need to have with the CoE member States' territories to require the applicability of these identified rights? It has to be recalled that this would happen under the final control of the European Court of Human Rights.[29]

To sum up, closely regarding the specificities of cloud computing technologies, contracting States to the ETS 108 have to determine which applicability of which national data protection rule to international cases is desirable and permitted and/or required, avoiding, on the one hand, suffocating a new technology and, on the other hand, depriving people under their jurisdiction of rights they already have or of new rights it is deemed appropriate they have.

18.9 Law Enforcements Agencies and Data Retention

The fact that CCS operators are processing huge amounts of data including quite sensitive ones about the CCS customers or third parties, explains the interest of law enforcement agencies to have access to these data through the CCS provider cooperation or by imposing this latter similar obligations than to public communication services operators as regards data retention imposed by the EU 2006 Directive on Data retention.[30] In other words, we have to pay attention to the question of the extension of certain legal obligations for certain communications services' providers to retain data about the uses of their services or to cooperate with law enforcement authorities at their request or even at their own initiative.[31] That obligation would be more or less similar to the obligation imposed by the EU Directive to the IAPs and publicly available e-communication services' operators. Other questions might be

---

[27] Regarding the potential influence of the ECHR on conflict of laws, see notably Gannagé, L. *"A propos de l' "absolutisme" des droits fondamentaux", in Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*. Paris: Dalloz, 2008, pp. 265–284.

[28] See European Court of Human Right, 20 July 2001, Pellegrini v. Italy.

[29] Mayer, P. "La Convention européenne des droits de l'homme et l'application des normes étrangères", *Revue Critique de droit international privé*, (1991): 664.

[30] 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.

[31] See the Council of Europe Cybercrime Convention, article 17.

raised. Cloud computing represents a shift of location which might have two consequences. The first one is the following: to what extent, can we consider that the LEA are authorised in case where data about a customer located in the LEA country are placed somewhere in the clouds to extend their searches to the foreign country where the data are located by the CCS and that using the online facilities offered to the customer? In line with this question we might pose the following: "Do the different national LEA'es have to cooperate together?"

Article 23 and ff of the Council of Europe Cybercrime Convention (art. 23 and ff) imposes such a duty to cooperate while fixing certain conditions of such cooperation and the means to ensure effectively that cooperation.

Within Europe, the 2009 Council Framework Decision on the European Evidence Warrant' "*for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters*"[32] imposes cooperation, but according to article 10 of the Decision, requires regarding the transfers of personal data, the consent of the executing authority, meaning the LEA which is required to transfer data to a LEA of another country. Beyond this text, other multilateral agreements serve as the basis for mutual assistance in criminal matters in the EU. We quote the Council of Europe Convention on Mutual Assistance in Criminal Matters, 1959 ("the 1959 Convention"), and its protocols of 1978 and 2001 and the Schengen Agreement of 1985 and the EU Convention on Mutual Assistance in Criminal Matters 2000 (the "MLAC"[33]) and its protocol of 2001.[34]

The second question represents the other facet of the distinction between the place of the data and the customer. "*Is a national LEA investigating the computer of a suspected person located in its territory allowed to extend the research outside of the country to information systems connected with the investigated computer*?" According to their criminal procedure legislations, certain national LEA (for instance, Belgium, UK and France) have this power to assert jurisdiction over data stored in other countries, but accessible via electronic networks located in their own country. So, if LEA is investigating in Belgium in a computer located in Belgium, LEA might capture data stored in a third country but accessible via the local system. With the same argument it would be possible for LEA investigating in CCS premises located in their country to enter into the whole CCS information system. In other

[32]The Council's 2009 Framework Decision on the European Evidence Warrant ("EEW") applies the mutual recognition principle to judicial decisions for the purpose of obtaining evidence for use in proceedings in criminal matters. The EEW provides that Member States' law enforcement authorities should give immediate effect to judicial search and seizure orders emanating from other Member States. The EEW also provides standard forms for issuing orders, and fixed deadlines for executing orders.

[33]We underline that he MLAC only binds those States that choose to ratify it. To date, the MLAC has been ratified by 23 of the 27 EU Member States.

[34]About all these texts and for a detailed commentary, Spencer, J.R. "The Problems of Trans-Border Evidence and European Initiatives to Resolve Them" (2007) 9 Cambridge Yearbook of European Legal Studies 477, at 478.

words, cloud service providers may be subject to disclosure requests in countries outside of those where the data are stored.

A third question is more delicate: Does a CCS provider have a legal duty to cooperate with LEA'es? Do we need a legal framework for this cooperation? The GNI (Global Network Initiative) [35] has developed voluntary guidelines as regards the response to be given to governments' demands for access or blocking as solutions to the multinational dimension of the problem? The GNI pleads notably:

- for a global consensus as regards the governmental demands (Who? How? For which offences? etc);
- for prohibiting any overbroad demand and need for clear communications by writing;
- for a narrow interpretation of the demand (e.g. limitation in principle to data concerning data subjects located within the country).

Furthermore, the signatories clearly announce that they will challenge governmental demand before the courts when these demands seem inconsistent with the legal requirements and that they will take appropriate measures to make the Information services' users aware of the policies followed by the CCS providers and the governments.

The recent US-EU SWIFT agreement approved by the EU Parliament in July, 6 2010[36] could also be evoked in this context since one might imagine that a foreign LEA would like to obtain data stored in Europe in order to discover certain evidence of criminal infringements. On that point in the context of this SWIFT case, the European Union and the US have signed a revised agreement on sharing banking data to investigate suspected terrorist financing, moving the long-running negotiations over the deal a step closer to completion. Under the revised deal, an EU official would be posted in the US treasury in Washington to scrutinize the transfer of the European banking data to investigators. Information requests are also to be "tailored as narrowly as possible" and will be checked by Europol, the EU's police coordination agency. This solution might be extended to the access of official authority to data stored in Europe by a CCS operator.

---

[35] See the principles adopted in 2008 "Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies, available at the GNI website: www.globalnetworkinitiative.org.
These Principles on Freedom of Expression and Privacy ("the Principles") have been developed by companies, investors, civil society organizations and academics. "*They are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR")*".

[36] http://register.consilium.europa.eu/pdf/en/10/st11/st11222-re01.en10.pdf

18.10 Conclusions

The main and initial question raised by the considerations and questions set above is whether specific regulation on cloud computing is needed.

At this stage, following the considerations provided in this chapter, it is clear that, from a privacy legal point of view, different cloud computing services have different characteristics: Facebook does not raise the same problems than Microsoft's Azure or Amazon's EC2.

On the one hand, services have different natures – e.g. IaaS, PaaS or SaaS, private or public clouds, etc, – and various purposes – domestic, professional, public, etc. And on the other hand, the involved actors are also very different – individuals who are consumers or professionals, SMEs, NPOs, administrations, worldwide corporations, etc, and numerous imbalances could exist between them. Therefore, the questions identified above could receive varying answers according to the many facets of cloud computing technologies that will most probably continually evolve. In fact, these facets not necessarily raise the same concerns as regards data protection. Moreover, in the same sense, these questions could also vary according to the particular services and actors at stake, and they could not always have the same pertinence.

The questions raised in this chapter can be summarised as follows:

(1) Is the differentiation between domestic use/non domestic use pertinent, and do we need to extend the protection to the legal person and to change the concept of personal data?

- As seen before, such modification would be needed in the new environment of Cloud computing which concerns individuals as well as legal bodies.
- By maintaining the exclusion of domestic use from the protection – as Directive 95/46 does – would exclude many individuals using cloud computing in a domestic way (social network, Email services, etc) from any protection. Is this acceptable?
- The notion of personal data is very narrow and is not including the know-how, the commercial secret, etc.

(2) Who are the actors of cloud computing? Do they need to be legally defined if it is not already the case? If they are already legally defined, do the definitions at stake need to be modified? We identified five, sometimes overlapping, categories of actors: subscribers, users, data subjects, controllers (co-controllers) and data processors. This raises two principal questions:

- Does the concept of data processor need to be defined under ETS 108?
- Do legal persons need to be protected under the data protection rules of the ETS 108, with regard to which data (extension of the definition of the personal data and, therefore, of the data subject)?

(3) Which existing duties under ETS 108 need to be adapted? Which non-existing duties under ETS 108 need to be created? As the case may be, which actor has to bear these modifications or these creations? More precisely:

- Should data processors have to support specific duties provided for by the law, and which duties (e.g. in general as regards transparence and liability)?
- Should co-controllers to be targeted by specific liability rules and a particular allocation of duties under ETS 108?
- Should a specific duty regarding security breaches be established? Who would have to support this new duty (provider and/or subscriber), towards which actor (subscriber and/or data subjects) and in which cases?
- How to treat the distinction between non-domestic and domestic processing activities? When is it still relevant and how to improve the protection of data subjects when a domestic use exception could apply (total exclusion of data protection law or establishment of a softer legal regime)?
- Should data retention obligations have to be imposed on cloud computing services providers, when and how?
- Due to the possible imbalance between the actors of the cloud, is consent always an adequate basis of the legitimacy of the processing at stake or should data controllers – and if so when – have a duty to base the legitimacy of their processing on an additional basis?

(4) How could what call the "data protection continuity" be maintained? This question can be subdivided into the following concerns:

- When the cloud computing service provider or its user (data subject) terminates the contractual relationship at stake, how can it be guaranteed that the data subject (user) will recover the total "ownership" (control) of data relating to him?
- In cases of bankruptcies, mergers of corporations or sales of corporations, etc, how can it be guaranteed that the level of protection originally ensured to the data subject will remain at least equivalent?

(5) How to face the numerous concerns arising out of the international character inherent in cloud computing? This broad question also needs to be sliced into parts:

- Do some specific cloud computing services (e.g., involving sensitive data) need to be forbidden when they imply TBDF between contracting States and, a fortiori, non-contracting States ensuring an adequate level of protection?
- Which concerns can be solved by binding corporate rules?
- How to assess the adequacy of non-contracting States to ETS 108 as regards the processing of personal data for law enforcement purposes?
- How far could consent and contract authorise TBDF outside the territories of contracting States, towards non-contracting States not ensuring an adequate level of protection?

- How to resolve conflict of laws when actors involved in the cloud are located anywhere in the world and rules on conflict resolution do not yet exist. In other words, we should work out rules to solve conflicts of law at least in the context of Cloud computing.
- Does the "territoriality" of data protection rules have to be differently defined depending on the duties (e.g. security or transparence) and the actors (data controller or data processor) at stake, and if so, how?
- Finally when their data are in the clouds how to ensure the protection of the data subjects against the investigatory powers of the LEA? Is there an obligation for CCS providers to cooperate with the different LEA? Is that allowed for a national LEA investigating in the computer of a suspected person located in its territory to extend the research outside of the country to information systems connected with the investigated computer? Is the "zoning of the net" possible and if yes can we impose it through appropriate regulations? Are the recent EU-US agreement about SWIFT a good point of departure as regards the fixation of the limits of the cooperation between LEA?

(6) Do we have to ban or restrict the use of cloud computing services regarding sensitive matters, professions or activities (public or not)?

- This question raises the issue to impose on the CCS provider to limit its cloud or country of storage to a certain area such as the European Union. It would avoid to have sensitive data stocked in a non democratic regime who would nor guarantee the respect of privacy.

(7) On the security field, do we need to make special provisions for the cloud computing?

- What's about the role of standardisation bodies?
- Do we need to envisage security breach provisions in that context?

References

Article 29 Data Protection Working Party, Working document on Privacy on the Internet – An integrated EU Approach to On-line Data Protection – (WP37), adopted on 21st November 2000

Article 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP56), adopted on 30 May 2002.

Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines (WP148), adopted on 4 April 2008.

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP169), adopted on 16 February 2010.

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (WP171), adopted on 22 June 2010, p. 17.

Blok, P. Het recht op privacy, Boom Juridische uitgevers, 2003.

Bygrave, L. *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague/London/New York: Kluwer Law International, 2002.

Gannagé, L. *"A propos de l' "absolutisme" des droits fondamentaux", in Vers de nouveaux équilibres entre ordres juridiques – Liber amicorum Hélène Gaudemet-Tallon*. Paris: Dalloz, 2008.

Gellman, B. Privacy in the clouds: Risks to Privacy and confidentiality from Cloud Computing, Report prepared for the World Privacy Forum, Feb. 23, 2009.

Kuner, C. "Data Protection Law and International Jurisdiction on the Internet", Parts 1 & 2, 18 (2 & 3). *International Journal of Law and Information Technology*, (2010).

Mayer, P. "La Convention européenne des droits de l'homme et l'application des normes étrangères", *Revue Critique de droit international privé*, (1991): 651–665.

Meil, P., and T. Grance. The NIST Definition of Cloud Computing, Version 15, 10-07-09, available on NIST (National Institute of Standards and Technology) web site.

Moiny, J.-P. "Facebook au regard des règles européennes concernant la protection des données", 2 E.C.J.L., 2010, pp. 235 and ff.

Reidenberg, J. "Technology and Internet Jurisdiction", 153 UNIV. OF PENN. L. REV. 1951 (2005).

Solove D.J. "Conceptualizing Privacy", 90 California Law Review, 2002, 1085-.

Spencer, J.R. "The Problems of Trans-Border Evidence and European Initiatives to Resolve Them" (2007) 9 Cambridge Yearbook of European Legal Studies 477.