NEWSLETTER
ICT, IP & Data Protection
2013
October

ELVINGER, HOSS & PRUSSEN
LUXEMBOURG LAW FIRM

CONTENTS

Articles

Best Practices

IN BRIEF

24 October 2013
In the context of the next "10x6" special ICT After Work talks, organised by PaperJam Business Club, Alexandre Fiévée will speak on the topic: "Is there a right of ownership over data?" (*Existe-t-il un droit de propriété sur les données?*)

PRESS REVIEWS

11 July 2013
Publication of an article entitled: "Outsourcing, Do not outsource its liability" in the business review, PaperJam Management, written on the basis of an interview with Alexandre Fiévée.
http://www.paperjam.lu/article/fr/ne-pas-externaliser-sa-responsabilite

06 June 2013
Following the publication of the 2012 annual report of the National Commission for Data Protection (*la Commission Nationale pour la Protection des Données*) on 10 July 2013, the newspaper, Luxemburger Wort, interviewed Alexandre Fiévée on the essential points of this report.
http://www.ehp.lu/uploads/media/Luxemburg_Wort_20130710_Wirtschaft_und_Finanzen.pdf

Articles

I. INFORMATION AND COMMUNICATION TECHNOLOGIES

1. FACEBOOK: WHAT RESPONSIBILITY?

The posting of comments on social networks, such as Facebook, may constitute a criminal offence, provided however those comments are considered "public".

In its press release of 6 September 2013, the Grand-Ducal Police, joined by the Prosecution Service, reiterated that certain activities on social networks "inciting violence against a specific individual", may result in sentencing pursuant to Article 22 (paragraph 3) of the amended Law of 8 June 2004 on freedom of expression in the media.

News item causes stir

This warning follows the posting, on the Facebook page "Go find the arsonist P." (*Aller trouver l'incendiaire P.*), of numerous editorial comments inciting people to commit a crime or a criminal offence against an individual who is from Portugal and domiciled in Luxembourg…This individual has been the subject, over the past few days, of a criminal investigation in Portugal because of his assumed involvement in an arson case.

It is in this context that the Prosecution Service and the Grand-Ducal Police reiterated that provocation to commit a crime or a criminal offence, even if it has no impact, is punishable by fines ranging from 500 euros to 5,000 euros and by a jail term of from eight days to one year, in application of Article 22 (paragraph 3) of the abovementioned law. According to the Luxembourg authorities, "individuals who perform such activities" should be careful as "being active on social networks does not guarantee anonymity".

Facebook goes beyond the private sphere

Such a warning may be surprising. Anonymity is not a matter for consideration. It is not because an individual carries out reprehensible activities anonymously that such behaviour is less reprehensible. Nonetheless, it is perfectly legitimate to draw the attention of Internet users to the fact that posting that kind of information on someone's Facebook page may be analysed as an offence.

Indeed, as opposed to what people might think, any post on a Facebook page is not necessarily private. And as soon as the comments in question are of a public nature, they may constitute a criminal offence.

This is the case of the comments in question, which may be analysed as having led to the committing of a crime or a criminal offence. They are reprehensible only if they have been made "available to the public" particularly "by means of media". Indeed, there must, within the meaning of the law on freedom of expression in the media, be a "post". This requirement is fulfilled each time disputed comments are made available to the greatest number of people.

Restricted or public dissemination?

Indeed, it appears from several rulings made in particular by the French courts that the public nature of a piece of information depends on its accessibility to Internet users. In a ruling dated 10 April 2013, the first civil chamber of the Court of Appeal considered that comments made by an individual on his/her Facebook page could not constitute public abuse (repressed by law), as they were made available only to "people accepted by the individual concerned, in a very limited number", who, as a result, formed a "community of interest". In this case, such

people were registered as "friends" or "contacts" of the account holder. In other words, the non-public nature shall be accepted each time that such comments are disseminated to only a limited number of members chosen by the person responsible for the Facebook page.

On the other hand, comments which may be qualified as inciting to commit a crime or a criminal offence, posted on a Facebook page accessible to anyone, or any such comments which may be seen by anyone on the "newsfeed" function accessible not only to friends but also to the "friends of friends", should therefore, pursuant to this case law, be considered reprehensible. It seems to be the case of the page "Go find the arsonist P." as it is public and accessible to anyone.

2. SHOULD ONE TRUST CONSUMER REVIEWS ON THE INTERNET?

The profusion of fake consumer reviews on the Internet has caused mistrust among Internet users. In order to restore their confidence, the AFNOR (French association for standardisation) issued a standard on 4 July 2013 "on online consumer reviews". But when will an international standard be issued?

Recent studies reveal that Internet users are more and more suspicious about the quality and the truthfulness of online information and have strong reservations regarding the issue of reliability of such alleged "consumer reviews" as posted on the websites of professionals. According to the 4th barometer et 83% of internet users of Internet users think that there are fake reviews among consumer reviews…(testntrust.fr)

This practice of fake consumer reviews is not new but the growing awareness of Internet users of the abuses by some professionals has caused a significant loss of confidence.

Because confidence and quality of service are necessary to create and develop a positive influence on the web (e-reputation), some players have been mobilising to establish, as part of a standard, "principles and requirements regarding collection, moderation and restitution processes of online consumer reviews". This resulted in the AFNOR standard NF Z 74-501, issued on 4 July 2013.

What is a standard?

A standard, which consists of a consensus between the stakeholders of a market or an industry, is a reference document defining the voluntary rules applicable to that market or industry. It must be approved by a standardisation institute. By defining a level of quality, security and compatibility, it aims at facilitating national and international trade. It is different from a regulation as it is not issued by public authorities: it demonstrates the commitment of the players in a market or in an industry to comply with a recognised and approved quality and security standard. The certification enables a third party (an independent body) to verify and attest to the completeness of the activity with the principles and requirements referred to in the standard. Whereas it is also possible to declare itself as complying with a standard, the false display of any such declaration can be analysed as a misleading commercial practice, which may render its author thereof liable.

What are these new principles and requirements?

The AFNOR Standard NF Z 74-50, issued on 4 July 2013, concerns all types of products and services (household appliances, insurance, catering, etc.) and all types of websites: websites of review collection, e-commerce websites.

The purpose of this standard is to ensure the primacy of the freshness of the reviews and of the transparency of the methods, pursuant to the following three processing steps:

- collection of the reviews, which shall be based, in particular, on:
  - the identification of the author of the review;
  - the personal experience of the author;
  - the need to be able to contact the author;
  - the prohibition from buying reviews;
  - the need to verify the personal experience.
- moderation of the reviews, which mainly implies:
  - actual transparency of the moderation rules in general terms and conditions of use of the website;
  - the impossibility to modify online reviews;
  - the requirement of a pre-moderation of the reviews (automatically or with human intervention);
  - the requirements of homogeneity in the moderation process.
- restitution and publication of the reviews, which imply, in particular:
  - observation of a chronological order, from the most recent to the oldest, to be observed;
  - the display of the whole reviews;
  - observation of a maximum publication period, from the issue by the consumer of his review.

A timely international standard

This standard helps, according to the AFNOR, "define confidence benchmarks" for Internet users. Of course, any web professional established in Luxembourg is given the opportunity to request certification on the basis of this standard. He or she may also, provided that he or she complies with the abovementioned principles and requirements, declare him/herself as observing this standard. But in any case, at the time of globalisation, an international standard, as part of the International Standardisation Organisation (ISO), would be timely. To be continued…

3. A NEW RIGHT OF CLAIM OF DATA IN THE CONTEXT OF OUTSOURCING

The Law amending Article 567 of the Commercial Code, awaited since last year, was finally voted on 9 July 2013 (the "**Law**"). This law substantially modifies Article 567 of the Commercial Code in order to adapt it to the new situations deriving from the latest technology developments.

Article 567 dealing with property claims in the case of a third party's bankruptcy now states that tangible and intangible fungible property in the bankrupt's possession at the time of the bankruptcy may be claimed by the person who has entrusted this property to the bankrupt or by their owner, provided that this property complies with certain requirements. Prior to that, only "goods", as tangible property, were subject to such a claim which,

consequently, cast into doubt the possibility for the owner to claim these data.

This reform comes at a time when offers of outsourcing (including cloud computing) are growing involving numerous data transfers towards third party providers or suppliers. Conscious of these new practices, Luxembourg wished to establish a favourable legal framework enabling, in particular, companies which choose to use this type of service to be assured of being able to claim their data in the case of bankruptcy of the provider or supplier.

The data can be claimed from the bankrupt provided that they can be separable from other intangible assets at the time of the bankruptcy. Which means, in the context of outsourcing services, that a company's data must be separable from the data of another company also hosted in the supplier servers.

This new right of claim can be analysed as a right of reversibility of data which had not previously been regulated by law. Nonetheless, this right of claim is only established for the moment in the event of bankruptcy of the depository. Companies can continue to claim their data pursuant to a reversibility clause, up to the end of the service contract, terminated for any reason whatsoever.

The Law can be viewed under: http://www.legilux.public.lu/leg/a/archives/2013/0124/a124.pdf

4. IP TRACKING UNDER STRICT SUPERVISION

Is the practice of IP tracking lawful? This is a system used by European travel companies to enable their prices to fluctuate in line with some Internet users' assumed interest in buying a ticket. The European Commission has been invited by Françoise Castex, MEP, to answer this question.

The commercial practice in question would consist of demanding a higher price for tickets than the price displayed when a user logged on to the company's website for the first time. The purpose thereof would be to prompt Internet users to purchase tickets immediately by giving them the impression that fewer tickets are now available and thus are more expensive.

From a technical point of view, this practice is made possible by the collection, when Internet users first visit a website, of their IP ("Internet Protocol") addresses as well as their browsing history, which thus enables the travel company, which is the publisher, to identify them later when they visit its website.

On 12 March 2013, the European Commissioner for Digital Data, Viviane Reding, who considered that "IP addresses […] [may] constitute personal data", answered that "without prejudice to the powers of the Commission […], national data protection supervisory authorities are the competent bodies to monitor the application of the national measures implementing Directive 95/46/EC". Thus, according to the Commission, it is up to the national supervisory authorities to ensure that the applicable provisions regarding data protection are complied with.

Regulated processing of data

All of the data protection supervisory authorities of the EU Member States agree that an IP address shall be considered as personal data. In this context, the publisher, who collects the IP address of a visitor, carries out a processing of data which is subject to the provisions of Directive 95/46/EC.

The publisher must then comply with certain conditions when performing such processing. The publisher must collect data for determined, explicit and legitimate purposes

and may not further process them for purposes incompatible with the purposes originally specified. In addition, any processing of data must be fair and lawful. The individual concerned must also be informed by, and give his/her consent to, the publisher.

Article 5 of Directive 2002/58/EC, which regulates the practice of cookies, could also be applied. Indeed, it is highly likely that, from a technical point of view, the practice of IP tracking is based on that of cookies.

In application of this text, the publisher who uses this practice would then also have to have the consent of the Internet user, which must be free, specific and informed.

Thus, by abstaining from complying with all or part of the abovementioned principles and conditions – resulting from Directive 95/46/EC and/or from Directive 2002/58/EC – the publisher, who uses the practice of IP tracking, would *de facto* be in breach.

Unfair commercial practice

The lawfulness of such practice must also be addressed on the basis of Directive 2005/29/EC, which prohibits unfair commercial practices, in particular misleading practices as they mislead the consumer particularly regarding "the availability" of the product or its "price".

It should be noted that in France the *Commission nationale de l'informatique et des libertés* (the data protection supervisory authority) reported that it works in partnership with the *Direction générale de la concurrence, de la consommation et de la répression des fraudes* ("***DGCCRF***") (Directorate-General for Competition, Consumer Affairs and Prevention of Fraud), in order to assess the needs for carrying out joint actions with the main companies concerned.

The Luxembourg data protection supervisory authorities (the "***CNPD***") have still not commented on the issue…

II. INTELLECTUAL PROPERTY

1. MAIN PROCEDURAL CHANGES AT BENELUX OFFICE FOR INTELLECTUAL PROPERTY

The Benelux Office for Intellectual Property ("**BOIP**") has taken decisions which will modify the Benelux Convention on Intellectual Property and its Implementing Regulations[1] in order to simplify, in particular, the trademark procedures. The main changes are detailed below. They have come into effect on 1 October 2013.

As regards trademarks, the main changes will relate to:

- **Languages.** The official languages of the BOIP will remain Dutch and French. However, it will be possible to use English as an additional working language. All BOIP procedures (including registration and opposition procedures) can potentially be carried out in English, provided that each party (in the case of opposition procedures for instance) agrees to use English.

- **Opposition procedure.** The two-month opposition period will be calculated from the date of publication of the trademark application and no longer from the first day of the month following the publication of the trademark application.

- **Trademark renewal procedure**. The procedure related to the renewal of trademark registrations will be simplified. The trademark registration renewal for another period of ten years will only be subject to the payment of the fees and no longer to a written request from the holder. The payment will be facilitated by the implementation of a tool on the BOIP's website.

- **E-filing of international trademark applications.** The BOIP, as a pilot office, now enables future trademark holders to file their international trademark applications electronically. Previously, a person who wanted to register an international trademark had to use a paper form.

In addition, the i-DEPOT service – used by creators since 1998 to prove the date of their creation (e.g. in case of counterfeiting) – will have a legal basis by being included and enshrined in the Benelux Convention on Intellectual Property.

[1] The Benelux Convention on Intellectual Property will be modified following the decision of the executive board of 22 July 2010; the Implementing Regulations under the Benelux Convention on Intellectual Property will be modified following the decision of the executive board of 21 and 22 June 2012 to repeal Protocol II of 8 December 2011 and to amend the Implementing Regulations, and by the decisions of the executive board of 22 March 2013 to amend the Implementing Regulations.

III. DATA PROTECTION

1. THE NOTIFICATION PROCEDURE OF PERSONAL DATA BREACHES

On 24 June 2013, European Commission adopted European Regulation 611/2013 regarding the measures applicable to the notification of personal data breaches under Directive 2002/58/EC (the "**Regulation**"), which came into force on 25 August 2013 and which is directly applicable in all Member States.[2]

Indeed, pursuant to Article 4 of Directive 2002/58/EC[3] ("**E-privacy Directive**"), "In the case of a personal data breach[4], the provider of publicly available electronic communications services shall, without undue delay notify the personal data breach to the competent national authority". In addition, "When the personal data is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay".

The E-privacy Directive is supplemented by this Regulation providing a strict legal framework in order to ensure coherent implementation of the technical measures related to personal data breaches across all Member States.

Notification to the competent national authority

The Regulation details the purpose of the notification, the period of notification and the information to be included in this notification. Thus, pursuant to Article 2 of the Regulation:

- all data breaches are concerned;
- the provider has to notify the personal data breach to the national authority no later than 24 hours after the detection of a personal data breach;
- the notification shall contain information regarding the identification of the provider, initial information on personal data breach, possible additional notification to subscribers and possible cross-border issues.

Moreover, the Regulation obliges national authorities to implement "electronic means for notification of personal data breaches and information on the procedures for its access and use."

In Luxembourg electronic communications service providers have been obliged to notify the National Data Protection Commission, *la Commission pour la protection des données,* (the "***CNPD***") of all personal data breaches which have occured in their systems since 2011.[5] In this regard, the *CNPD* did not wait for the Regulation to come into force to implement an electronic procedure enabling

[2] This means that in the case of a conflict between the regulation and Luxembourg law for instance, the regulation will prevail.

[3] The Directive 2002/58/EC has been amended by the Directive 2009/136/EC of 25 November 2009 modifying, in particular, Article 4 in respect to "Security processing".

[4] Pursuant to Article 1(i) of the Directive 2002/58/EC: « personal data breach means 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."

[5] The "E-privacy Directive", as amended (see footnote 3) was effectively transposed into Luxembourg Law of 28 July 2011 modifying the Law of 30 May 2005 regarding electronic communications.

the providers to proceed with this notification. Indeed, the *CNPD* provides an electronic form which is available on its website. However, it falls, now, to the *CNPD* to supplement this form in order to comply with the new requirements covered by the abovementioned Regulation and to enhance the information related to this notification in order for the providers to have easier access and use of it.

Notification to the subscriber or the individual

In certain cases, providers have to notify the subscriber or the individual of a personal data breach when it is "likely to adversely affect the personal data or privacy". This notification shall be made without undue delay.

The Regulation provides an exemption to this principle and specifies that, in certain circumstances, the provider is able to postpone the notification to the subscriber or the individual upon the agreement of the national authority. Indeed, when personal data breaches require investigation, and when the notification to the subscriber or the individual "may put at risk the proper investigation of the personal data breach" such as criminal investigation, the disclosure to the subscriber or the individual by the provider may be postponed.

2. PRISM PROGRAM UNDER EUROPEAN SURVEILLANCE

On 13 August 2013, the Article 29 Working Party seized the European Commission in order to obtain clarification on the US program called "Prism" and its impacts on the protection of the personal data of European citizens.

Since the disclosures, last June, of Edward Snowden, former CIA computer specialist and contractor for the NSA, on the electronic spying of the NSA (US National Security Agency), many articles have been published on this topic and explanations have been provided by the US authorities. There are still grey areas and, in particular, regarding the issue of the protection of the personal data of European citizens. It is in this context that, on 13 August 2013, the Article 29 Working Party sent a letter to the Vice-president of the European Commission, Viviane Reding (in charge of the reform on data protection in Europe), so that the Commission could obtain answers from the US authorities to several questions. This working party was implemented by Article 29 of Directive 95/46/EC constituted by the representatives of all national authorities for data protection (including the *CNPD* for Luxembourg).

Disclosures

On 6 and 7 June 2013, the Guardian and the Washington Post disclosed certain practices implemented by the NSA with respect to the surveillance of electronic communications (Internet and mobile phones) used by individuals but also by European embassies and States. The computer program Prism is at stake. Prism is apparently an advanced search engine allowing the NSA to collect a very high number of data from, in particular, electronic communications with the participation of *inter alia* Google and Facebook. (see Facebook's likely response to its involvement: Privacy: 1st Facebook report)

Apparently the NSA also uses another tool – Xkeyscore – which, from the abovementioned data, would allow cross-referencing and, thus, the obtaining of even more precise information on individuals and/or on institutions (search history of a user on the Internet, identification of all the individuals speaking a determined language in a considered country, etc.).

According to the US Government, such a surveillance system is perfectly lawful: it is a program that collects information under

judicial supervision – regarding non-US citizens and is performed with the assistance of electronic service providers – in application of Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Amendment Act ("**FISA**").

Questions

In its letter, the Article 29 Working Party expresses its wish that the European Commission should, in the context of an investigation, determine which type of information is precisely affected by this system and which are the precautions taken regarding the access and the collection performed by the US authorities. In this respect, the Working party would like to know if data are collected on European territory or if such collecting is limited to data hosted on US servers. In other words, this is a question asked of the US authorities on what they consider data localised on US territory, knowing that many of them only use this territory in transit without being physically available or hosted there.

The other clarification requested by the Article 29 Working Party deals with the conditions under which the judicial authority (FISA Court) is seized and the criteria it uses to authorise the surveillance of individuals. The goal of the Working Party is, on the one hand, to understand what type of goal followed by the US authorities may justify such a breach of individual rights and, on the other hand, to assess whether the performed data processing is in line with the principles of personal data protection as laid down by international law and European law.

Another question was raised. It regards the possibility for the supervised individuals to claim their rights (appeals) before the relevant US authorities. In this respect, the Article 29 Working Party underlines that if these individuals are not informed that they are the subject of investigations, they cannot challenge the collected data and express their views.

Finally, the Article 29 Working party would like this investigation to be extended to the whole European territory in order to determine whether similar programs have been implemented by Members States and whether, if they have, they are consistent with the rules in force regarding personal data protection.

At this time, it appears that the European Commission has still not reacted to this seizure. To be continued…

3. 2012 ACTIVITY REPORT OF CNPD: RESULTS, EXPECTATIONS AND PROSPECTS

The 2012 activity report was presented on 2 July 2013 at a press conference in Esch-Belval and is now available on the website of the *Commission Nationale de Protection des Données* ("***CNPD"***).

This independent authority – established as a public institution – has been the watchdog of the fundamental rights relating to the processing of personal data for 10 years (any information regarding an identified or identifiable individual) and is taking stock of the year 2012 which it regards as "very active" and is providing us with the main actions it intends to carry out in the "coming years".

Results

- Review of previous formalities

Numbers to remember.

Reported processing operations (any operation relating to personal data) number 18,659, with a total of 1,362 (notifications + authorisation applications) for the year 2012. Such operations were carried out by 5,821

reporting agents/controllers, located in Luxembourg.

The number of notifications, i.e. 586, has increased compared to 2011, and 80% thereof come from players of the private sector. Notifications mainly concern processing operations of staff administration, human resources management, customer management, accounting and supplier management.

As a result of their entailing a particular risk as regards the privacy of individuals, certain processing operations must be subject to the *CNPD*'s prior approval (processing operations relating to supervision, processing of biometric data, processing of genetic data, transfer of data outside the European Union with an inappropriate protection level, etc.). In 2012, 706 authorisation applications were examined by the Commission.

They mainly related to supervision and geolocation processing operations. In addition, 48 applications were submitted to obtain the *CNPD*'s authorisation for transferring data to third countries (outside the European Union), which is the same as last year, but way more than 10 years ago. Indeed, according to the *CNPD*, "the development of commercial transactions and globalisation have led to (…) a dramatic increase in the number of transfers of personal data with respect to projects of centralisation and outsourcing of staff, customer or supplier management, as well as when they outsource their IT activities".

It should be noted that in 2012, most of these applications were from firms in the financial industry and to the United States and India.
Unfortunately the Commission does not report how it has replied to such applications and what might have caused it to dismiss them, as the case may be…

- Review of complaints

In 2012 the *CNPD* received and investigated 133 complaints (i.e. 15 % more than in 2011) from individuals considering themselves aggrieved by a controller: unobserved requests for data deletion or correction; access denied to data in breach of the right of access to which any individual though is entitled; transfer of data to an unauthorised third party (e.g.: an NGO which has transferred data to a marketing agency without the consent of the relevant individuals); non-effective exercise of the right to refuse to receive SPAM; sending of SPAMs without the recipients' prior consent.

According to the *CNPD*, the high number of complaints reveals "the citizens' increasing concern about the protection of their data".

- Data protection officers

It should be noted that only 68 reporting persons have appointed data protection officers. A data protection officer is, in application of the law, an independent person who has power of investigation inside the firm, for the purpose of ensuring the supervision of the compliance with the law and a right of information with this firm.

It seems that the *CNPD* regrets that controllers do not work more with such data protection officers, the institution of which constitutes "a big step in developing the data protection culture in the firms and organisations in question which will have the necessary in-house knowledge and expertise".

In this regard, the Commission states that the proposed European Regulations on data protection, which are being examined by the European parliament, require the appointment of a data protection officer inside each entity of a certain size or depending on the particular nature of the

processed data… it being specified that, in application of Luxembourg law, any such data protection officer may be a chartered accountant, an auditor but also a lawyer.

The expected reform

According to the *CNPD*, the purpose of the proposed European Regulation of 25 January 2012 (which will replace Directive 95/46/CE) is to enhance data protection "by offering citizens the opportunity to better control what happens to their data, by making data holders more responsible, by making the implementation of legal provisions related thereto more efficient and by strengthening the powers of the supervisory authorities".

The final text should be adopted by early 2014 and enter into force two years later.

Prospects

The "ultimate" goal announced by the *CNPD* is to "strengthen the trust of citizens and consumers in the attitude of players who collect and use information concerning them". Within this context, it shows a very strong will to "boost the culture of data protection in Luxembourg and compliance with the rights of the individuals concerned". Various means will thus be implemented "over the coming years", including the strengthening of "investigations and controls on site". According to the *CNPD*, such means "will now play a more important role among the provided forms of assistance" in order to "strengthen compliance with the rights of individuals".

Indeed, in application of the law of 2002, the Commission has a power of investigation pursuant to which it has access to data which are processed. It may, in this context, collect "all information necessary" for the performance of its supervision duties. For that purpose, it has direct access to the premises where processing operations take place and carries out the "necessary verifications". Through such visits, it may check the lawfulness of performed processing operations either on its own initiative, or in the continuation of a complaint. It also focuses, traditionally every two years, on a "considerable investigation" in an area giving rise to large or particularly sensitive data processing operations (which had been the case for the telecommunications sector, in the late 2000s).

In 2012 the Commission carried out 18 controls and investigations, in particular with respect to complaints regarding video surveillance. The main cases related to either cameras installed by individuals filming nearby properties or the public road, or cameras installed by the employer in the workplace.

The Commission has not reported whether it was to carry out some "considerable investigation" regarding a specific sector in 2013.

One thing is sure; it intends to take advantage of the next three years before the texts being debated in the European Parliament and in the Council enter into force, to prepare for this new environment. It requests private players, in particular "entities of a certain size" and those for which the "nature" of their activities justifies it, to carry out a certain number of actions: appoint and train an "in-house data protection officer", perfect the identification and examination of processes and processing operations and review the system security. It should be noted that public players will also be involved so that they can prepare for "taking on their responsibility" more "proactively".

And what if the 2013-2014 "considerable investigation" concerned such various categories of players, namely on the one hand, private players "of a certain size" and

players for which the "nature" of their activities justifies it, and on the other hand, the public sector?

4. PROCESSOR BINDING CORPORATE RULES, A NEW LEGAL INSTRUMENT IN FAVOUR OF THE CLOUD

Considering that the existing supervisory measures regarding transfers outside the European Union are not sufficiently adapted to all outsourcing situations (and notably Cloud computing), the Article 29 Working party is suggesting the use of processor Binding Corporate Rules ("**BCR**").

This legal instrument is intended for service suppliers ("**processors**") carrying out transactions on behalf of their clients ("**data controllers**"), the performance of some of which involve international data transfers to other entities of their group.

Thus, the processor BCR can be analysed as an internal code of conduct which defines the policy of a group regarding personal data transfers, which thereby constitutes a safe harbour for transfers made by a processor to other processors of the same group.

This instrument may be very helpful in the event of an agreement entered into by a client ("**data controller**") and a Cloud computing service provider (processor established on the territory of the European Union), the performance of which involves certain services to be provided outside the European Union by other companies of the same group as the supplier.

Indeed, for the data controller, such a legal document:

- shall constitute a guarantee that transfers are carried out in accordance with the principles of Directive 95/46/EC (in this respect, the BCR are to be annexed to the processing contract);
- shall enable him or her to avoid entering into as many contracts as there are transfers within the group of the processor;
- shall guarantee that he or she receives transfer authorisations from the national data protection authorities.

For the processor, the BCR will enable him:

- to standardise practices regarding data protection within the group;
- to communicate on the business policy regarding data protection with the clients and ensure a satisfactory protection level.

The first step for the service providers concerned will consist of appointing a national data protection authority called "leader" (such as the *CNPD* which will then be in charge of the cooperation procedure with the authorities of the other concerned European countries) and in providing it with the registration form.

In order to help these companies to implement these BCR, the Article 29 Working party adopted a document on 19 April 2013 specifying the main items which should be contained therein.

Best Practices

WEB 2.0: MANAGE YOUR E-REPUTATION

The company's e-reputation is the image that internet users have about this company on the basis of information found on Internet, and in particularly on blogs and social networks. Indeed, the company's e-reputation depends on several factors: articles published online, consumers' reviews and sometimes… staff's behaviours. To prevent unwanted behaviours:

1. *Staff must always keep in mind:*

   - Once in the public eye, always in the public eye;
   - Our obligations in the physical world are the same in the digital world;
   - Spoken words fly away, written words remain.

2. *Make your staff aware of digital common sense:*

   - Do not disclose any information on the internet that you would not personally share with anyone;
   - Do not infringe third party rights;
   - Behave on the internet as you would at work;
   - Separate "talking about yourself", "talking about your company" and "speaking on behalf of your company";
   - Enter into a conversation, it's sharing constructive criticisms and accepting criticisms;
   - Be careful of the buzz effect.

3. *For these purposes, the company may use an e-reputation charter and the services of a community manager.*