The revolution in social analysis due to Big Data and their predictive capacities poses different questions related to risks of asymmetries in the control over information. In order to have access to this technology and to exploit its power, it is necessary to have the availability of large data sets and to invest heavily in equipment and research. Only governments and big companies have these resources and, consequently, are able to exercise such control over digital information both to enhance their performances and to enhance their control over individuals. Considering the role of government agencies and their increasing requests of information to the private sector for public security purposes, it appears necessary to adopt specific rules in order to regulate the information flow, to define the rights over data and to ensure adequate enforcement. If it is true that information is often publicly available, it is also true that the line between the public and private sphere will become even more blurred in the Big Data era. After a brief introduction (I.) this article first outlines the new scenario of Big Data (II.) before analyzing the governments’ interplay with private entities which crucially enhances their social control (III.). Finally, the currently envisaged changes by the EU reform on data protection are scrutinized in their potential effects on the future of social control (IV.).

I. Introduction

The recent NSA case1 is just the latest in a series of programs adopted by governmental agencies in various nations to pursue massive social control; nevertheless, it has sparked a wide debate about data protection and social control. Many opinions have been voiced that comparison between the U.S. and European data protection standards and have expressed conflicting considerations about the level of protection guaranteed by different countries. However, in many cases, intelligence activities have little to do with general data protection regulations, since they are authorized by specific legislative provisions introducing exceptions to general principles.2 Nevertheless, regulations on data protection and

---


privacy play a relevant role in these intelligence activities, mainly in terms of indirect limitation.

In western democratic nations, the modern social control is no longer realized only by intelligence apparatus, which autonomously collects a huge amount of information through pervasive monitoring systems. The social control is the result of the interaction between the private and public sector, based on a collaborative model made possible by mandatory disclosure orders issued by courts or administrative bodies and extended to an undefined pool of voluntary or proactive collaborations from big companies.\(^4\)

In this way, governments obtain information with the indirect “co-operation” of the users who probably would not have given the same information to public entities if requested. Service providers for example collect personal data in the case of private agreements (privacy policies) with the consent of the user and for their specific purposes,\(^5\) but governments exploit this practice by using mandatory orders to obtain the disclosure of this information. This dual mechanism hides from citizens the risk and the dimension of the social control that can be realised by monitoring social networks or other services and using Big Data analytics technologies.

From this perspective, with regard to the programs carried out by government agencies and their increasing requests of information to the private sector for public security purposes, it is necessary to consider the role which data protection regulations can assume in terms of reduction of the amount of data collected by private entities, increasing the minimization and, consequently, have an indirect impact on the information available for purposes of public social control.

II. The New Scenario of Big Data

Historically, regulations have to define the border between actions with a positive social output, which are permitted and induced by laws, and antisocial behaviours, which are prohibited and punished. This function is also served by the law in an ICT context and regulations on data protection represent a clear example of the role assumed by the law in shaping the use of new technologies and technologies themselves.

In doing so, the law can use traditional “behavioural” rules, which permit or prohibit certain activities by using a three-phase model focused on prescription, ex post evaluation and sanction. This traditional model is efficient in contexts where individual activities are traceable and the identity of the author of illicit activities can be discovered. However, these conditions are not always present in on-line dimensions or they involve excessive costs. For this reason, a different approach based on the embedding of legal prescription into the design of technological devices and processes represents a good alternative.\(^6\) Law-orientated technologies offer more advantages in terms of enforcement and application in international contexts. Thus, shaping technologies in order to create a “structural” barrier to possible illicit uses should ultimately reduce unlawful behaviours. The implementation of technology-based solutions is also less conditioned by the local legal framework than the implementation of “behavioural” solutions and could easily be realized uniformly in different legal systems. For these reasons, in many cases this approach is more suitable than ordinary “behavioural” rules to address the transnational dimension and the continuous evolutionary aspects of ICT regulation.

These considerations can be made with regard to the Big Data context and can help in addressing the challenges that it poses to the existing legal framework in terms of autonomy of individuals (user’s self-determination), groups or populations (social control).

1. Technological Capabilities

Big Data is not something new, but currently at the final stage of a long evolution of the capability to analyse data using computer resources. Big Data represents the convergence of different existing technologies that permit enormous data-centres to be built, create high-speed electronic highways and have ubiquitous and on-demand network access to computing resources (cloud computing). These technologies offer substantially unlimited storage, allow the transfer of huge amounts of data from one place to another and allow the same data to be spread in different places and re-aggregated in a matter of seconds.

All these resources permit a large amount of information from different sources to be collected. The whole dataset can be continuously monitored in order to identify the emerging trends in the flows of data. This approach is revolutionary and differs from the traditional sampling method, which is based on the extraction of a representative sample from the total statistical population.

However, in order to define the sample it is necessary to define in advance the purposes of the research and some working hypotheses. In this sense traditional sampling methods show their limits because they tend to infer or imagine the relevant aspects to be examined, so unexpected tendencies may not be considered. On the contrary, using Big Data analytics, new trends become self-explanatory and the purposes are necessarily defined in advance but are a consequence of monitoring the flows of data. In this sense, unlike the traditional method, the Big Data approach focuses on the tendencies which emerge from collected information. It uses an inductive method which requires the largest amount of information possible, as it is not possible to select a representative sample in an analysis that does not start out with a precise target of study. This method involves a

---


2. Competitive Advantage for Few Players Only

The availability of these new technologies gives a competitive advantage to those who own them in terms of capability to predict new economic, social and political trends. The information and knowledge deriving from Big Data is not accessible to everyone, as it is based on the availability of large datasets, expensive technologies and specific human skills to develop sophisticated systems of analyses and interpretation. For these reasons, governments and big business are in the best position to take advantage of Big Data: they have large amounts of information on citizens and consumers and enough human and computing resources to manage it.

Another relevant aspect of the control deriving from Big Data is the amount of it. Analyses focused on profiling enable to predict the attitudes and decisions of any single user and even to match similar profiles. In contrast, Big Data is not used to focus on individuals, but to analyse large groups and populations; Big Data analytics do not predict the next book that the man in the street will read, but the political sentiment of an entire country.

This control is all the more pervasive when it is realised by government agencies in countries where legal provisions grant them the power to require information about individual citizens from private companies in order to realise an invasive and generalized monitoring of the behaviour of thousands of people. The results are rather peculiar as, in this way, governments obtain information with the indirect “co-operation” of the users. Those users probably would not have given the same information to public entities if requested. Service providers for example collect personal data on the base of private agreements (privacy policies) with the consent of the user and for their own purposes, but governments exploit this practice and use mandatory orders to obtain the disclosure of information. This dual mechanism hides from citizens the risk and the dimension of the social control that can be realized by monitoring social networks or other services.

3. Resulting Asymmetry

For these reasons, the existing context is characterized by an asymmetric distribution of control over information, which has an impact on social control that is not counterbalanced by the traditional pillars of data protection, the purpose limitation principle and the “notice and consent” model. The complexity of data processes and the power of modern analytics drastically limit the awareness of data subjects, their capability to evaluate the various consequences of their choices and the expression of a real free and informed consent. This lack of awareness is not avoided by giving adequate information to the data subjects or by privacy policies, due to the fact that these notices are read only by a very limited number of users who, in many cases, are not able to understand part of the legal terms usually used in these notices.

These aspects are even more relevant in a Big Data context rendering the traditional model of data protection to be in crisis. The traditional model is based on general prohibition plus “notice and consent” and the coherence of the data collection with the purposes defined at the moment in which the information is collected. However, nowadays much of the value of personal information is not apparent when noticed and present are normally given and the “transformative” use of Big Data makes it often impossible to explain the description of all its possible uses at the time of initial collection.

Various commentators consider that the privacy risks related to Big Data analytics are low, pointing out the large amount of data processed by analytics and the de-identified nature of most of this data. This conclusion is wrong; Anonymity by de-identification is a difficult goal to achieve, as demonstrated in a number of studies.

12 With regard to personal information collected by public entities the Directive 95/46/EC permits the data collection without the consent of data subject in various cases; however, the notice to data subjects is necessary also in these cases. See Articles 7, 8 and 10, Directive 95/46/EC.
13 See Cate, F H and Mayer-Schonberg, V (2012), 3, above at fn. 11.
The power of Big Data analytics to draw unpredictable inference from information undermines many strategies based on de-identification. In many cases a reverse process in order to identify individuals is possible; it is also possible to identify them using originally anonymous data. Here, it is closer to the truth to affirm that each data is a piece of personal information than to assert that it is possible to manage data in a de-identified way.

For these reasons, the study of the existing interaction between public and private social control and the analysis of specific forms in which it is realised represent the first step in order to define an answer to these social and legal challenges.

III. Public and Private Interplay in Social Control

The interaction between public and private in social control could be divided in two categories, both of which are significant with regard to data protection. The first concerns the collection of private company data by government and judicial authorities (see 1. below), whilst the second is the use by government and judicial authorities of instruments and technologies provided by private companies for organisational and investigative purposes (see 3. below).

1. Array of Approved eSurveillance Legislation

With regard to the first category and especially when the request is made by governmental agencies, the issue of the possible violation of fundamental rights becomes more delicate. The Echelon Interception System and the Total Information Awareness (TIA) Program are concrete examples which are not isolated incidents, but undoubtedly the NSA case has clearly shown how could be invasive the surveillance in the era of global data flows and Big Data. To better understand the case, it’s quite important to have an overview of the considerable amount of electronic surveillance legislation which, particularly in the wake of 9/11, has been approved in the US and, to a certain extent, in a number of European countries.

The most important legislation is the Foreign Intelligence Surveillance Act (FISA) of 1978 which lays down the procedures for collecting foreign intelligence information through the electronic surveillance of communications for homeland security purposes. The section 702 of FISA Act amended in 2008 (FAA) extended its scope beyond interception of communications to include any data in public cloud computing as well. Furthermore, this section clearly indicates that two different regimes of data processing and protection exist for US citizens and residents (“USPERs”) on the one hand, and non-US citizens and residents (“non-USPERs”) on the other. More specifically the Fourth Amendment is applicable only for US citizens as there is an absence of any cognizable privacy rights for “non-US persons” under FISA.

Thanks to FISA Act and the amendment of 2008, US authorities have the possibility to access and process personal data of EU citizens on a large scale via, among others, the National Security Agency’s (NSA) warrantless wiretapping of cable-bound internet traffic (UPSTREAM) and direct access to the personal data stored in the servers of US-based private companies such as Microsoft, Yahoo, Google, Apple, Facebook or Skype (PRISM), through cross-database search programmes such as X-KEYSCORE. US authorities have also the power to compel disclosure of cryptographic keys, including the SSL keys used to secure data-in-transit by major search engines, social networks, webmail portals, and Cloud services in general (BULLRUN Programme).

It’s important to underline that there is a legal framework between the EU-US Mutual Legal Assistance Agreement (MLAA) ratified by the EU and the US Congress on October 2003 permitting collaboration that covers criminal investigations, and counter-terrorism activities in search of evidence for law enforcement purposes. However, it’s not yet clear, whether US authorities respect this agreement in their surveillance operations.

Even if the FISA Act is the mostly applied and known legislative tool to conduct intelligence activities, there are other relevant pieces of legislation on electronic surveillance. One need only to consider the Communications Assistance for Law Enforcement Act (CALEA) of 1994, which authorises the law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance. Furthermore, following the Patriot Act of 2001, a plethora of bill has been proposed. The most recent bills (not yet in force) are the Cyber Intelligence Sharing and Protection Act (CISPA) of 2013, which would allow Internet traffic information to be shared between the U.S. government and certain technology and manufacturing companies and the Protecting Children From Internet Pornography Act.


See Bowden, C (2013), 13, above at fn. 22.


See Communications Assistance for Law Enforcement Act (18 USC § 2522).

The “Dark Side” of Big Data: Private and Public Interaction in Social Surveillance

Although there exist legal frameworks that empower law enforcement to access data, we have also empowered law enforcement33, which extends data retention duties to US Internet Service Providers.

Truthfully, the surveillance programmes are not only in US. In Europe, the Communications Capabilities Development Programme has prompted a huge amount of controversy, given its intention to create a ubiquitous mass surveillance scheme for the United Kingdom in relation to phone calls, text messages and emails and extending to logging communications on social media. More recently, on June 2013 the so called programme TEMPORA showed that UK intelligence agency Government Communications Headquarters (GCHQ) has cooperated with the NSA in surveillance and spying activities. These revelations were followed in September 2013 by reports focusing on the activities of Sweden’s National Defense Radio Establishment (FRA). Similar projects for the large-scale interception of telecommunications data by both France’s General Directorate for External Security (DGSE) and Germany’s Federal Intelligence Service (BDE).

Even if it seems that EU and US surveillance programs are similar, there is one important difference: In the EU, under Data Protection law, individuals have always control of their own personal data while in US, the individual have a more limited control once the user has subscribed to the terms and condition of a service.

2. Forced “On Call” Collaboration by Private Entities

Other than government agencies’ monitoring activities, there are cases in which Internet Service Providers collaborate spontaneously or over a simple request from the law enforcement agencies. The exponential increase in Big Data since 2001 has provided a truly unique opportunity. In this respect, a key role has been played by Social Media. One need only reflect on the fact that Facebook, Twitter, Google+ and Instagram, all of which are situated in Silicon Valley, boast around 2 billion users throughout the world and many of these users are citizens of the European Union. Facebook’s founder may have intended to “empower the individual,” but there is no doubt that Social Network Services (SNSs) have also empowered law enforcement33, which extends data retention duties to US Internet Service Providers.

To stay on the topic of information acquisition by the law enforcement, there are two interesting cases of the collection of Big Data for crime prevention purposes:

The first is the “PredPol” software initially used by the Los Angeles police force and now by other police forces in the USA (Palm Beach, Memphis, Chicago, Minneapolis and Dallas). Predictive policing, in essence, cross check data, places and techniques of recent crimes with disparate sources, analysing them and then using the results to anticipate, prevent and respond more effectively to future crime. Even if the software house created by Predpol declares that no profiling activities are carried out, it becomes essential to carefully understand the technology used to anonymize the personal data acquired by the law enforcement database. This type of software is bound to have a major impact in the US on the conception of the protection of rights under the Fourth Amendment, and more specifically on concepts such as “probable cause” and “reasonable suspicion” which in future may come to depend on an algorithm rather than human choice.

The second example is X1 Social Discovery software. This software maps a given location, such as a certain block within a city or even an entire particular metropolitan area, and searches the entire public Twitter feed to identify any geo-located tweets in the past three days (sometimes longer) within that specific area. This application can provide particularly useful data for the purpose of social control. One can imagine the possibility to have useful elements (e.g. IP address) to identify the subjects present in a given area during a serious car accident or a terrorist attack.

b) Legitimacy

From a strictly legal standpoint, these social control tools may be employed by gathering information from citizens directly due the following principle of public:

“Where someone does an act in public, the observance and recording of that act will ordinarily not give rise to an expectation of privacy”.

In the European Union, whilst this type of data collection frequently takes place, it could be in contrast with ECHR case law which, in the Rotaru vs. Romania

27 Protecting Children From Internet Pornographers Act of 2011.
31 See United States v. Miller (425 US 425 [1976]). In this case the United States Supreme Court held that the “bank records of a customer’s account are the business records of the banks and that the customer can assert neither ownership nor possession of those records”. The same principle could be applied to an Internet Service Provider.
36 See http://www.x1discovery.com/social_discovery.html.
case,38 ruled that “public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities”. As O’Floinn observes: “Non-private information can become private information depending on its retention and use. The accumulation of information is likely to result in the obtaining of private information about that person”39.

In the US, this subject has been addressed in the case People v. Harris40, currently pending in front of the Supreme Court. On January 26, 2012, the New York County District Attorney’s Office sent a subpoena to Twitter, Inc. seeking to obtain the Twitter records of user suspected of having participated in the “Occupy Wall Street” movement. Twitter refused to provide the law enforcement officers with the information requested and sought to quash the subpoena. The Criminal Court of New York confirmed the application made by the New York County District Attorney’s Office, rejecting the arguments put forward by Twitter, stating that tweets are, by definition, public, and that a warrant is not required in order to compel Twitter to disclose them. The District Attorney’s Office argued that the “third party disclosure” doctrine put forward for the first time in United States v. Miller was applicable41.

3. Use of Private Sector Tools and Resources

The second relationship concerns the use by the state of tools and resources from the private company for the purposes of organisation and investigations. Given the vast oceans of big data, US governmental authorities decided to turn to the private sector, not only for purposes of software management but also in relation to management of the data itself. One example is the CTO’s Hadoop platform42, which is capable of memorizing and storing data in relation to many law enforcement authorities in US. Similarly, a private cloud system has emerged which conveys the latest intelligence information in near-real time to U.S. troops stationed in Afghanistan43. Another example is the facial recognition technology developed by Walt Disney for its park and sold to the US military force44.

Considering costs saving and massive computing power of a centralized cloud system, it is inevitable that law enforcement, military forces and government agencies will progressively rely on this type of services. The aforementioned change will entail deductible legal issues in terms of jurisdiction, security and privacy regarding data management. The relevant legal issues might be solved through a private cloud within the State with exclusive customer key control. However, it is worth considering that, in this way, private entities will gain access to a highly important and ever expanding information asset. Therefore, they will be able to develop increasingly sophisticated and data mining tools, thanks to cloud systems’ potential. This scenario, which is already a fact in the USA, might become reality also thanks to the impulse of the Digital Agenda for Europe and its promotion of Public Private Partnership initiatives on Cloud45. This is why it is important that European cloud services should be based on high standards of data protection, security, interoperability and transparency about service levels and government access to information as it has recently been recognized by the European Commission46.

IV. The EU Reform on Data Protection

The framework described above shows that modern social control is the result of the interaction between the private and public sector. This collaborative model is not only based on mandatory disclosure orders issued by courts or administrative bodies, but has also extended to a more indefinite grey area of voluntary and proactive collaboration by big companies. It is difficult to get detailed information on this second model of voluntary collaboration; however, the predominance of US companies in the ICT sector, particularly with regard to the internet and cloud services, increases the influence of the US administration on national companies and makes specific secret agreements of cooperation in social control easier47.

Against this background, the political and strategic value of the European rules on data protection emerges. These rules may assume the role of a protective barrier in order to prevent and limit access to the information about European citizens and companies48. In this sense, the EU Proposal for a General Data Protection Regulation49 extends its territorial scope50 through “the pro-

41 See United States v. Miller (425 US 425 [1976]).
48 Although only regarding natural persons are under the European regulation on data protection, the data concerning clients, suppliers, employees, shareholders and managers have a relevant strategic value in competition.
50 See Article 3 (2), Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Compromise amendments on Articles 1–29 (here-

Exemplar für Alessandro Mantelero
cessing of personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of such data subjects.”51

1. Relevance for Social Control

Although the Proposal for a new regulation does not regard the data processed by public authorities for the purposes of prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties52, its impact on social control is significant, since in many cases the databases of private companies are targeted by public authority investigations. For this reason, reducing the amount of data collected by private entities and increasing data subjects’ self-determination with regard to their personal information limit the possibility of subsequent social control initiatives by government agencies.

However, the complexity of data processes and the unclear wording of many privacy policies53 along with the presence of technological and market lock-in effects reduces data subjects’ awareness of the consequences of their consent and facilitate the creation of a wider database which is only accessible by the authorities in cases provided by the law.

The EU Proposal, in order to reinforce the protection of individual information, interacts with these constraints and shifts the focus of data protection from an individual choice towards a privacy-oriented architecture54. This approach, which limits the amount of data collected through “structural” barriers and introduces a preventive data protection assessment55, also produces a direct effect on social control by reducing the amount of information available.

2. Reinforcing the Individual’s Self-Determination

With regard to the information collected, the EU Proposal reinforces users’ self-determination by requiring data portability, which gives the user the right to obtain a copy of the data undergoing processing from the controller “in an electronic and structured format which is commonly used and allows for further use by the data subject”56. Portability will reduce the risk of technological lock-in due to the technological standards and data formats adopted by service providers, which limit the migration from one service to another.

However, in many cases (e.g. Facebook, Google, Twitter, etc.), the services offered by Big Data owners, which generate these massive collections of information, are worldwide services provided by a very limited number of companies. In terms of social control, this situation reduces the chances for users not to be tracked by moving their account from one platform to another and, thereby, minimises the positive effects of data portability.

Finally, the Proposal reinforces the right to obtain the erasure of data processed without the consent of the data subject, against his objection, without providing adequate information for him or outside of the legal framework57. An effective implementation of this right can reduce the overall amount of data stored by service providers, and may limit the amount of information existing in the archives without a legitimate reason for the processing of information. In this manner, the possibility of consulting the history of individual profiles by authorities is also reduced.

All the aspects considered above concur to limit the information available to all entities interested in social control, and therefore, also affect the request of disclosure held by government agencies and courts to private companies. Nevertheless, these powers of search and seizure and their exercise represent the fundamental core of social control.

3. Trans-Border Data Flow for Private Entities

In order to analyse this aspect in the scenario of the future European data protection framework it is necessary to consider both proposals by the European Commission:

- the Proposal for a new General Data Protection Regulation (GDPR)58 and
- the less debated Proposal for a Directive in the law enforcement sector (PDPI)59

Although the second proposal is more specific on governmental and judicial control, the first considers this aspect from the point of view of the data flows.

The new proposal, as well as the currently in force Directive 96/46/EC, allows trans-border data flows from the EU to other countries only when the third country provides an adequate level of data protection60. When evaluating the adequacy of data protection in a given country...

---

51 In other abbreviated as PGDPR-LIBE_1-29, available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/comp_am_art_01-29en.pdf See also Article 3 (2), PGDPR.
52 See also Recital 21, PGDPR and Recital 21, PGDPR-LIBE_1-29.
53 This area will fall under the new Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25 January 2012 (hereinafter abbreviated as PDPI), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:COM:2012:0016:FIN:EN:PDF; see the Explanatory Memorandum of the Proposal.
54 See above § 1.
58 See above fn. 49.
59 See above fn. 52.
try, the Commission should also consider to the legislation in force in third countries “including concerning public security, defence, national security and criminal law”61. Consequently, the presence of invasive investigative public bodies and the lack of adequate guarantees to the data subject assume relevance for the decision whether to limit the trans-border data flows between subsidiaries and holdings or between companies. Once again, this limit does not affect public authorities, does not restrict the set of information held by private companies available for their scrutiny.

4. Effects of Trans-Border Data Flow Rules on Social Control

Without considering the NSA case that is still on-going, an explanatory case on the relationship between trans-border data flows, foreign jurisdiction and the possible effects on citizens and social control is provided by the SWIFT case; the same criticism applies and has been expressed by commentators with regard to the US Patriot Act. These two cases differ because in the NSA case non-EU authorities requested to access information held by a company based in the EU, whereas in the SWIFT case the requests were directed to US companies in order to have access to the information they received from their EU subsidiaries.

a) Current Legitimacy of Data Disclosure

In the SWIFT case62 the Article 29 Data Protection Working Party clarified that a foreign law does not represent the legal base for the disclosure of personal information to non-EU authorities, since only the international instruments provide an appropriate legal framework enabling international cooperation63. Furthermore, the exception provided by Art. 26 (1) (b) Directive 95/46/EC64 does not apply when the transfer is not necessary or legally required on important public interest grounds of an EU Member State65.

In contrast (as emerged in the PATRIOT Act case and also with reference to the wider, complex and dynamic system of powers enjoyed by the U.S. government in the realm of criminal investigations and national security66), the US authorities may access data held by the EU subsidiaries of US companies67. However, it is necessary to point out that there is a potential breach of protection of personal data of European citizens and that this happens not only with regards to US laws, but also in relations with other foreign regulations, as demonstrated by the recent draft of the Indian Privacy (Protection) Bill68 and Chinese laws on data protection69.

b) Approach by Proposed Data Protection Regulation

In order to reduce such intrusions the draft version of the EU Proposal for a General Data Protection Regulation limits the disclosure to foreign authorities and provides that “no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State”70.

The draft also obliges controllers and processors to notify national supervisory authorities of any such requests and to obtain prior authorisation for the transfer by the supervisory authority71. These provisions had been dropped from the final version of the Commission’s Proposal on 25 January 2012, but have now been reintroduced by the European Parliament, as a reaction to the NSA case72.

---

61 See Article 41 (2) (a), PGDPR-LIBE_30–91 and also Art. 41 (2) (a), PGDPR.
64 Art. 26 (1) (b) justifies the transfer that is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (Article 26 (1) (d) of the Directive.
65 See also Article 29 Data Protection Working Party, ‘Opinion 10/2006’, 25, above fn. 62 “(any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Directive”).
67 It is necessary to underline that the guarantees provided by the U.S. Constitution in the event of U.S. government requests for information do not apply to European citizens, as well as, legal protection under specific U.S. laws applies primarily to U.S. citizens and residents.
70 See Art. 42 (1), Proposal for a General Data Protection Regulation, draft Version 56, November 29th 2011.
72 See Article 43a, PGDPR-LIBE_30–91. This provision does not clearly
5. Limiting Violations of EU Citizen’s Privacy

In addition to the Proposal for a General Data Protection Regulation, the above mentioned Directive on the protection of individuals with regard to the processing of personal data by competent authorities establishes some protection against a possible violation of EU citizens’ privacy.

The goal of this Directive is to ensure that “in a global society characterised by rapid technological change where information exchange knows no borders” the fundamental right to data protection is consistently protected. One of the main issues at EU level is the lack of harmonisation across Member States’ data protection law and even more “in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations”. Whilst a directive may not have the same impact on harmonising national regulations currently in force in various Member States, it does in fact represent the first piece of legislation to have direct effect when compared to the previous attempts by way of Council of Europe Recommendation No. R (87) and Framework Decision 2008/977/JHA.

The founding principles of this Directive, which are shared with the previous directives referred to, are two-fold:

(1) First there is the need for fair, lawful and adequate data processing during criminal investigations or to prevent a crime, on the basis of which every data must be collected for specified, explicit and legitimate purposes and must be erased or rectified without delay.

(2) Then there is the obligation to make a clear distinction between the various categories of the possible data subjects in a criminal proceeding (persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, persons convicted, victims of criminal offense, third parties to the criminal offence).

For each of these categories there must be a different adequate level of attention on data protection, especially for persons who do not fall within any of the categories referred above.

These two principles are of considerable importance, although their application on a practical level will be neither easy nor immediate in certain Member States: This is easily demonstrated by the difficulties encountered when either drafting practical rules distinguishing between several categories of potential data subjects within the papers on a court file, or attempting to identify the principle on the basis of which a certain court document is to be erased.

In addition to these two general principles the provisions of the Directive, are interesting and confirm consolidated data protection principles. Sufficient to mention here the prohibition on using measures solely based on automated processing of personal data which significantly affect or produce an adverse legal effect for the data subject, as well as the implementation of data protection by design and by default mechanisms to ensure the protection of the data subject’s rights and the processing of only those personal data.

Furthermore, the proposal for a Directive in the law enforcement sector entails the obligation to designate a data protection officer in all law enforcement agencies in order to monitor the implementation and application of the policies on the protection of personal data.

These principles constitute a significant limitation to possible data mining of personal and sensitive data collection by law enforcement agencies. If it is true that most of these provisions were also present in the Recommendation No. R (87) of Council of Europe and in the Framework Decision 2008/977/JHA, it is also true that compelling data protection by design and by default mechanisms and measures could encourage data anonymisation and help to avoid the indiscriminate use of automated processing of personal data.

V. Conclusion

The increasing adoption of social surveillance programmes by government agencies and their development based on interaction with private databases probably requires a different regulatory approach, one which acts both on the data collection process carried out by private companies and on access to and use of personal information by government agencies and law enforcement.

In this respect, data protection regulations can play an important role in terms of reducing the amount of data collected by private entities and, consequently, having an indirect impact on the information available for purposes of public social control. The EU Proposal for a General Data Protection Regulation, at least, seems to respond to this challenge.

To complete the protection of citizens against the risks of social control, it is also necessary to regulate and control the use of personal information acquired for law enforcement purposes; in this sense the EU proposal for a Directive in the law enforcement sector represents the first attempt to harmonise and strengthen citizens’ guarantees.

76 Recommendation No. R (87) 15 regulating the use of personal data in the police sector.
78 Art. 4, PDPI and Art. 4b PDPI-LIBE.
79 Art. 5, PDPI-LIBE.
80 Art. 9a, PDPS-LIBE.
81 Art. 19, PDPI.
82 Art. 30, PDPI.
Electronic Patient Records and eHealth – Current Legal Developments in Switzerland

How best to arrange relevant medical patient data in the digital age?

Within the greater scheme of the “eHealth Switzerland Strategy”, the introduction of electronic patient records (so-called “ePatientrecords”) gains key importance. An electronic patient record provides treatment-relevant medical data, which can be accessed by authorized persons (patients and health care professionals) swisswide and any time by using automated processes. The establishment of such an electronic patient record is optional, but given the sensitive health data contained in these records particular importance has to be placed on privacy and data security matters.

This paper will, after a glance at the eHealth strategy Switzerland (I.) and the potential of eHealth applications (II.), critically look at the Swiss Draft Bill on Electronic Patient Records which has recently been submitted to the Swiss parliament.

1. eHealth Switzerland Strategy

“The people in Switzerland may grant, in the field of health care and to health care professionals of their choice, access to relevant information about themselves irrespective of place and time. They are actively involved in decisions regarding their health and their health problems and thus strengthen their health literacy. Information and communication technologies are to be used in a way that the networking of healthcare actors is ensured and that the processes are of better quality, more safe and efficient.”

These words outline the strategic vision on which the implementation of eHealth structures in Switzerland relies. Among the – almost generic – term “eHealth” or “e-Health” the bunch of information and communication technologies (ICT) is subsumed and used to design, support and integrate various processes and participants in health care. This is primarily done to simplify and link established processes. Most frequently eHealth applications are used in the areas of administration, information, consultation, diagnosis, prescription, referral, treatment, monitoring and accounting.

2. Preliminary Proposal and Explanatory Report

On 27 June 2007, the Confederation and the cantons jointly developed the “eHealth Switzerland Strategy”. This strategy covers the period from 2008 to 2015 and was formally adopted by the Federal Council. This is to ensure that all people in Switzerland will have access to an affordable and high in quality, efficient and safe operating health care service. The strategy highlights how the identified cornerstones are to be inserted in the future and thereby defines three priority areas for action to be realised:

1. The electronic patient records: Concerning electronic patient records the strategic goal was set that the Swiss population shall, by the end of 2015, be enabled to grant service providers of their choice electronic access to treatment-relevant information.

2. The Online Services: In the same timeline shall the online services be operating and thereby establishing a health portal with secure access through that the people may access their own electronic patient record coupled with the ability to retrieve structured and specific information.

3. The implementation of the “eHealth Strategy”: Thirdly, the implementation of the “eHealth Strategy” is about the definition of those organisational, legal and technical measures that are essential for the development of eHealth applications in Switzerland.

In order to ensure the successful implementation of the “eHealth Switzerland Strategy” the so-called “Expert Group eHealth” was set up with the task to clarify the necessity of relevant legal regulation. The final report with recommendations was published end of September 2010. As a result, the “Expert Group eHealth” proposed, among other things, to focus on the primary purpose of electronic patient records, namely the support and optimization of patient treatment, to allow for a no obligation to participate in electronic patient records for patients and health professionals (so-called “double voluntariness”) and to provide and ensure interoperability as well as enforcement of privacy and security.

2. Preliminary Proposal and Explanatory Report

Following the recommendations of the “Expert Group eHealth”, the Federal Council mandated the Federal Department of Home Affairs with the task to develop both a preliminary proposal and an explanatory report...